



INFORMACJA PRASOWA

Każda próba podszycia się pod ZUS to przestępstwo

Oszustwa są ścigane z urzędu, a wyłudzenie pieniędzy jest zagrożone karą od 6 miesięcy do 8 lat pozbawienia wolności – przypomina Zakład Ubezpieczeń Społecznych. Oszuści wymyślają coraz to bardziej wyrafinowane metody działań. Stąd też apel ZUS do klientów, by byli ostrożni i nie dali się nabrać na manipulacje przestępców.

- W ostatnich tygodniach wyraźnie wzrosła liczba oszustów, którzy podszywają się pod pracowników ZUS, przysyłając fałszywe wiadomości (przez e-mail, SMS-y czy komunikatory internetowe tj. Messenger czy WhatsApp) lub podejmując kontakt telefoniczny. Celem takich działań jest wyłudzenie danych osobowych, informacji o rachunkach bankowych bądź skłonienie do otwarcia niebezpiecznych linków lub załączników – mówi Beata Kopczyńska, regionalna rzeczniczka prasowa ZUS w województwie śląskim.

Apele o ostrożność to za mało. Oszuści stosują coraz bardziej wyrafinowane technicznie i psychologicznie metody perswazji, a ich katalog rośnie praktycznie każdego dnia. Dlatego ściśle współpracujemy z Policją i wszelkimi innymi instytucjami zwalczającymi zwłaszcza cyberprzestępczość wymierzoną w osoby starsze. ZUS cieszy się zaufaniem klientów. Wysyłane przez przestępców fałszywe wiadomości SMS lub e-mail, które dotyczą np. zwiększenia emerytury, zmiany numeru telefonu czy rzekomych zmian dokonanych na Platformie Usług Elektronicznych (PUE)/eZUS to nie tylko działanie na szkodę klientów, ale także Zakładu.

Pamiętaj, że ZUS nigdy:

- nie prosi o podanie danych osobowych drogą mailową, SMS-ową lub za pomocą wiadomości poprzez komunikatory internetowe,
- nie wysyła linków do logowania ani do weryfikacji danych przez wiadomości tekstowe,
- nie wysyła umów ani formularzy do wpłaty na rachunki inwestycyjne,
- nie nakłania do wykonywania przelewów na wskazane konto bankowe.

W razie jakichkolwiek wątpliwości zadzwoń do Centrum Kontaktu Klientów ZUS pod numer 22 560 16 00. Infolinia jest czynna od poniedziałku do piątku od 7:00 do 18:00.

– Naszym klientom przypominamy: zanim zrobicie cokolwiek, najpierw skontaktujcie się z nami telefonicznie lub osobiście w placówce. Pośpiech jest w tym przypadku złym doradcą, a przestępcy umiejętnie wywierają presję, bo wiedzą, że jeśli klient najpierw zadzwoni do nas, to oszustwo się nie powiedzie – dodaje rzeczniczka.

Niewyczerpany katalog pomysłów na oszustwa

W ostatnim czasie oszuści podszywający się pod pracowników ZUS są bardzo aktywni. Najczęściej chodzi im o pozyskanie numeru PESEL, numeru konta bankowego oraz danych logowania (np. do poczty elektronicznej czy bankowości internetowej). Przestępcy mogą również próbować wyłudzić pieniądze.

Próby oszustów przybierają różne formy, przykładowo:

- oszuści pojawiający się w domu

Podająca się za pracownika ZUS kobieta odwiedzała domy naszych klientów. Oszustka proponowała pomoc w wypełnianiu wniosków dotyczących m.in. przejścia na emeryturę czy uzyskania bonu turystycznego. Ważne! Wizyty pracowników poza siedzibami jednostek ZUS odbywają się jedynie w ściśle określonych przypadkach. To kontrola prawidłowości wykorzystania zwolnień lekarskich. Drugim przypadkiem wizyt jest kontrola przeprowadzana u osób prowadzących pozarolniczą działalność gospodarczą. Kontrolę taką prowadzą wyłącznie inspektorzy kontroli na podstawie upoważnienia. Co ważne kontrola jest zawsze zapowiadana wcześniej.

- fałszywe wiadomości rozsyłane różnymi kanałami w celu wyłudzenia danych

Do klientów wysyłano wiadomości o zmianie kanału odzyskiwania dostępu do profilu na PUE/eZUS. Zawierały w załączniku „plik logowania” (na przykład z rozszerzeniem .xll). Fałszywe maile wyglądają wiarygodnie – mogą zawierać domenę „zus.pl” w adresie nadawcy oraz dane przypominające prawdziwy login PUE/eZUS. Do klientów wysyłane są także wiadomości od osób podających się za „pracowników Działu Świadczeń czy Emerytur”, w związku z „projektem” dotyczącym dodatkowego zarobku i zwiększenia otrzymanej emerytury. W kolejnym etapie klienci są proszeni o dokonanie przelewu na dane z fałszywej umowy, którą otrzymali. Ważne! ZUS nie wysyła do swoich klientów korespondencji e-mailowej. Kontakt elektroniczny ze strony Zakładu możliwy jest jedynie w sytuacji, gdy klient ma profil na PUE/eZUS i wyraził zgodę na taką formę kontaktu.

- oszuści telefoniczni

Osoby podszywające się pod pracowników Zakładu dzwonią i proszą o potwierdzenie zmiany numeru telefonu w ZUS lub na PUE/eZUS. Często rozmowy dotyczą instytucji finansowych, z których korzystają klienci. Ważne! Konsultanci infolinii ZUS nie dzwonią do klientów w sprawie zmiany numerów telefonów do konta na PUE/eZUS czy zmiany numerów telefonów w bankach.

- fałszywe profile ZUS w mediach społecznościowych/komunikatorach

W mediach społecznościowych pojawiają się spreparowane konta ZUS oraz fałszywe reklamy.

Rozpowszechniają one nieprawdziwe informacje, np. o rzekomych inwestycjach, które zagwarantują emeryturę już w wieku 50 lat lub pozwolą zwiększyć kwotę już pobieranego świadczenia. Oszuści twierdzą, że wystarczy zainwestować już 500 zł, żeby uzyskać dodatkowe pieniądze.

Ważne! ZUS nie wysyła do swoich klientów e-maili z umowami, prośbami o podanie danych kart kredytowych ani nie zachęca do otwierania plików i linków.

Co zrobić, gdy otrzymasz podejrzaną wiadomość?

- Nie podawajmy nikomu poufnych informacji, zwłaszcza po otrzymaniu podejrzanych wiadomości (komunikator, e-mail czy SMS) zawierających prośbę o udostępnienie danych. Nie klikajmy też w podejrzaną linki – ani e-mailowe, ani przesyłane w wiadomościach SMS lub komunikatorach. I jeszcze jedna ważna sprawa – uwaga na załączniki, nie pobierajmy ich jeśli nadawca wzbudza nasze wątpliwości, podejrzenia, nie znamy go – radzi rzeczniczka.

Jeżeli mamy wątpliwości co do tożsamości osoby, która podaje się za pracownika ZUS, skontaktujmy się z najbliższą placówką ZUS lub zadzwoń do Centrum Kontaktu Klientów pod numer 22 560 16 00.

Beata Kopczyńska
regionalna rzeczniczka prasowa ZUS
w województwie śląskim