Warszawa, 30.03.2022 r.

INFORMACJA PRASOWA

**SMS lub mail o nadpłacie podatku? Uważaj, to może być oszustwo**

**Informacja z Urzędu Skarbowego o tym, że mamy do odebrania nadpłatę podatku, to z pewnością dobra wiadomość. Za to powiadomienie o niedopłacie, może wpędzić każdego w poważne zaniepokojenie. Kiedy dostaniemy SMS-a na ten temat, powinniśmy mieć się na baczności – to może być próba oszustwa - ostrzegają eksperci Biura Informacji Kredytowej.**

Zeznanie podatkowe za rok 2021 można złożyć pomiędzy 15 lutego a 2 maja. Mimo, że na roczne rozliczenie podatku mamy ponad 3 miesiące, nawet milion osób co roku pozostawia ten obowiązek na ostatnią chwilę, załatwiając go w pośpiechu. Szczególnie w takiej sytuacji łatwo stracić czujność.

Według danych Ministerstwa Finansów i Krajowej Administracji Skarbowej prawie 20 mln osób (19,6 mln PIT-ów) rozliczyło się w ubiegłym roku z podatku elektronicznie. Wygoda i coraz większe przekonanie do całkowicie zdalnego załatwiania spraw urzędowych, decydują o wyborze usług elektronicznych. Wykorzystują to przestępcy, którzy licząc na nasze zaufanie do instytucji publicznych, podszywają się pod nie, aby ukraść nasze pieniądze.

**Przestępstwo na nadpłacony podatek**

Z roku na rok liczba przestępstw związanych z podszywaniem się pod instytucje zaufania publicznego systematycznie wzrasta. Oszuści podszywają się pod pracowników banków, policję, pracowników służby zdrowia zajmujących się programem szczepień, czy w końcu urzędników skarbowych.

Każdy, kto posiada numer telefonu komórkowego, może dostać SMS-a od rzekomego urzędnika Urzędu Skarbowego z informacją, że ma nadpłatę podatku lub na jego koncie powstała zaległość.

W celu uregulowania powstałej zaległości podany jest link rzekomo prowadzący do konta urzędu lub zalecenie skontaktowania się z przedstawicielem skarbówki, np. pod podany numer telefonu komórkowego.

O tym, że nie powinno się klikać w takie linki, słyszał już niemal każdy. Dlatego oszuści rozwijają kolejne metody, by wykraść nasze dane osobowe i pieniądze.

**Oszustwo na podatnika – nowy sposób na wyłudzenie danych i pieniędzy**

Wszystkie przypadki podszywania się pod instytucje publiczne łączy cecha wspólna. Narażają klientów na utratę zaufania, np. do swojego banku oraz dążą do wyłudzenia środków finansowych. Sposoby przestępców ewoluują, z roku na rok modyfikowane są schematy działań socjotechnicznych.

*- Wcześniej przestępcy przesyłali SMS-em link, kierujący do fałszywej strony popularnych operatorów płatności, za pośrednictwem którego ofiara miała zalogować się do swojego banku, aby otrzymać zwrot nadpłaconego podatku lub pokryć niedopłatę. W ten sposób oszuści przejmowali dostęp do konta i zgromadzonych na nim pieniędzy. Dziś wiele osób już wie, że nie należy klikać w żadne linki otrzymane w sms lub w mailu. Dlatego przestępcy zmieniają taktykę, coraz bardziej operując socjotechniką* - mówi Maciej Wójcik, Starszy Specjalista w Zespole Cyberbezpieczeństwa, Biura Informacji Kredytowej.

Jak wskazują eksperci BIK, nowy sposób działania oszustów polega już nie na przesłaniu linku, ale numeru telefonu do urzędnika, czyli na uwiarygodnieniu tego kontaktu.

*- Obecnie przestępcy nakłaniają w wiadomości sms do skontaktowania się z fałszywym urzędnikiem Urzędu Skarbowego, który pomoże im w załatwieniu sprawy. Przez telefon „żywa” osoba instruuje dzwoniącego, jak pobrać odpowiednie oprogramowanie do weryfikacji tożsamości lub w celu ułatwienia zapłacenia określonej kwoty na odpowiednie konto. Wszystko po to, aby tak, jak w poprzednich scenariuszach, uzyskać dostęp do rachunku bankowego* - tłumaczy Maciej Wójcik.

Kiedy przestępca uzyska dostęp do konta ofiary może nie tylko „wyczyścić” jej konto, ale pójść o krok dalej – na przykład zaciągnąć w jej imieniu kredyt, z którego pieniądze również przejmie.

**Nie daj się nabrać - fiskus nigdy nie poprosi o żadne dane przez telefon**

Urzędy Skarbowe nie kontaktują się za pośrednictwem SMS-ów, maili czy telefonu, by prosić o podanie wrażliwych danych, na przykład do zalogowania się do bankowości elektronicznej. Skarbówka wysyła oficjalną korespondencję do podatników listem poleconym lub poprzez korespondencję na specjalnym portalu usług publicznych – ePUAP.

Zwrot podatku może być dostarczony na trzy sposoby: pocztą, na numer konta bankowego lub osobiście w kasie urzędu skarbowego. O formie decydujemy na etapie wypełniania rocznego zeznania PIT, wypełniając dedykowaną temu sekcję

- *Cyberprzestępcy są coraz bardziej kreatywni i lepiej zorganizowani. Ich metody ewoluują, wykorzystują ludzką naiwność, obliczone są na błąd, najczęściej popełniany w pośpiechu. Dlatego, by uniknąć oszustw, należy kierować się zasadą ograniczonego zaufania. Nie tylko nie należy klikać w linki, ale również nie wolno instalować żadnego oprogramowania, gdy ktoś prosi nas o to przez telefon. W takiej sytuacji najlepiej się po prostu rozłączyć. W celu weryfikacji sprawy, np. wymagającej uiszczenia opłaty, wystarczy samemu skontaktować z daną instytucją, korzystając z numeru lub adresu podanego na oficjalnej stronie urzędu* – radzi Maciej Wójcik z BIK.

Roczne rozliczenie podatkowe to obowiązek, przed którym staje każdy z nas. Choć mamy na to sporo czasu, to wielu z nas przypomina sobie o tym tuż przed 30 kwietnia i w pośpiechu wypełnia formularze PIT. Może to generować niepotrzebne nerwy lub co gorsza pomyłki, na które czyhają przestępcy.

W pośpiechu łatwiej przeoczyć niepokojące sygnały, np. próby wyłudzenia naszych danych osobowych i pieniędzy. Ustawowy termin na złożenie PIT za 2021 rok dla większości osób fizycznych upływa 30 kwietnia, ale ponieważ w 2022 r. ten dzień wypada w sobotę, to możemy rozliczyć się w tym roku do 2 maja.

**Eksperci BIK zalecają zachowanie zdrowego rozsądku we wszystkich sprawach, które dotyczą danych osobowych. Ponadto wskazują, jak zadbać o swoje dane tożsamości i zabezpieczyć się przed wyłudzeniem.** Należy sprawdzić, czy:

* masz konto na [www.bik.pl](http://www.bik.pl) – może wówczas bezpłatnie zastrzec swój dowód osobisty w przypadku jego utraty lub kradzieży zawartych na nim Twoich danych;
* korzystasz 24/7 z ochrony przed wyłudzeniami – Alertów BIK - dostaniesz powiadomienie, gdy ktoś złoży wniosek o kredyt, pożyczkę lub będzie próbował podpisać umowę z usługodawcą w Twoim imieniu. Dodatkowo co miesiąc otrzymasz potwierdzenie, że wszystko jest ok i BIK nie odnotował potencjalnych prób wyłudzenia na Twoje dane;
* znasz adres [www.bik.pl/wsparcie](http://www.bik.pl/wsparcie) i wiesz, jak pomóc osobie, na którą wyłudzono kredyt lub sam masz takie podejrzenie. Pod tym adresem znajdziesz wsparcie w weryfikacji sprawy, pomoc w zgłoszeniu na policję i do instytucji, w której doszło do wyłudzenia.

**Biuro Informacji Kredytowej S.A.** – jedyne biuro kredytowe w Polsce, które poprzez internetowy portal [www.bik.pl](http://www.bik.pl) oraz aplikację mobilną [Mój BIK](https://www.bik.pl/moj-bik) umożliwia klientom indywidualnym monitorowanie własnej historii kredytowej, a dzięki [Alertom BIK](https://www.bik.pl/klienci-indywidualni/alerty-bik?utm_source=gazeta.pl&utm_medium=artykul&utm_campaign=alerty) ostrzega przed każdą próbą wyłudzenia kredytu. BIK gromadzi i udostępnia dane o historii kredytowej klientów indywidualnych i przedsiębiorców z całego rynku kredytowego, oraz dane z obszaru pożyczek pozabankowych. Baza BIK zawiera informacje o 164 mln rachunków należących do 25 mln klientów indywidualnych oraz 1,4 mln firm, w tym o 845 tys. mikroprzedsiębiorców prowadzących działalność gospodarczą. BIK posiada najwyższe kompetencje w zakresie [Analiz rynkowych](https://media.bik.pl/analizy-rynkowe) i nowoczesnych technologii. Wspiera bezpieczeństwo instytucji finansowych i ich klientów, udostępniając bezpieczny system wymiany informacji kredytowych i gospodarczych oraz nowatorskie rozwiązania antyfraudowe. Łączy cechy nowoczesnej firmy technologicznej z atrybutami instytucji zaufania publicznego. Od kilkunastu lat BIK jest aktywnym członkiem międzynarodowego Stowarzyszenia ACCIS, zrzeszającego największą grupę rejestrów kredytowych na świecie.

|  |  |
| --- | --- |
| **Kontakt dla mediów:****Aleksandra Stankiewicz-Billewicz**Biuro prasowe BIK tel.: + 48 22 348 4131kom.: + 48 512 164 131aleksandra.stankiewicz-billewicz@bik.pl  |  |