Warszawa, 21.04.2023 r.

INFORMACJA PRASOWA
…………………………………….

**Coraz więcej ataków phishingowych - uwaga na fikcyjne komunikaty
o „zwrocie podatku”**

**Zagrożenie phishingiem cały czas rośnie, uważają Polacy. Już niemal 7 na 10 ankietowanych obawia się, że oszuści podszyją się pod jakąś instytucję albo osobę, a oni w dobrej wierze odpowiedzą
i przekażą im swoje dane czy dostęp do konta – wynika z realizowanego dla BIK badania „Cyberbezpieczeństwo Polaków”. Okres składania rocznych zeznań podatkowych to dla cyberprzestępców dodatkowa, świetna okazja do nasilenia ataków z wykorzystaniem tej oszukańczej techniki. W tym czasie udają administrację skarbową i robią to na dużą skalę,
bo z wyłudzaniem „na PIT” spotkało się w ubiegłym roku aż 15 proc. Polaków.**

Wykorzystywanie wizerunku Urzędu Skarbowego to typowy przykład kampanii phishingowej – potwierdza NASK, Państwowy Instytut Badawczy. Ataki z wykorzystaniem tej metody nasilają się zwłaszcza w okresie zbliżającego się terminu rozliczenia rocznych zeznań podatkowych. Dlatego, bardzo ważna jest ostrożność i unikanie podawania swoich danych w reakcji na sms lub telefon
o rzekomej nadpłacie lub niedopłacie podatku. Celem cyberprzestępców nie jest pomoc, lecz kradzież pieniędzy.

Rodacy zdają sobie sprawę z czyhających zagrożeń. Z regularnie realizowanego dla BIK badania „Cyberbezpieczeństwo Polaków” wynika, że według ankietowanych **w największym stopniu nasiliło się zagrożenie wyłudzeniami metodą podszywania się pod instytucję publiczną (68 proc) oraz zagrożenie phishingiem (68 proc.).** Od jesieni do wiosny odsetek ankietowanych obawiających się phishingu wzrósł z 60 do 68 proc. Z próbami wyłudzeń na PIT, kontaktem w sprawie nadpłaty lub niedopłaty podatku zetknęła się w poprzednim roku całkiem spora grupa osób, 15 proc. badanych. Ale prób wyłudzenia z wykorzystaniem phishingu doświadczył już co trzeci ankietowany.

**O co chodzi w phishingu**

Z roku na rok oszuści usprawniają swoje metody przestępcze i coraz częściej łączą technologię z socjotechniką. Bez względu jednak na zastosowaną taktykę, schemat jest ten sam. Chodzi o to, by ofiara uwierzyła, że ma do czynienia z prawdziwą instytucją i kliknęła w link bądź ściągnęła sugerowaną aplikację. W ten sposób przestępcy mogą przechwycić jej dane osobowe albo przedostać się do systemu transakcyjnego jej konta.

*- Typowe przypadki wyłudzeń to przede wszystkim manipulacja socjotechniczna w rozmowie telefonicznej, w której oszust podszywa się pod pracowników banku, firmy telekomunikacyjnej, policji, znanej instytucji finansowej czy firmy, wywołująca u rozmówcy poczucie zagrożenia, strach. W takiej sytuacji jesteśmy skłonni do podania wrażliwych danych osobom, które oferują nam pomoc* – tłumaczy**Andrzej Karpiński, dyrektor Departamentu Bezpieczeństwa Grupy BIK**.

Niekiedy już nawet część danych wystarczy do podjęcia próby zaciągnięcia kredytu czy podpisania umowy abonamentowej z dostawcą usług telekomunikacyjnych na cudze nazwisko. Drogiego smartfona przestępcy otrzymają za złotówkę i sprzedadzą, a operator będzie oczekiwał, że ofiara przez dwa lata będzie opłacać rachunki.

*- Przestępcom nie zależy, aby proceder szybko wyszedł na jaw, więc mogą podać wymyślony adres do korespondencji. Nie dowiemy się prędko, że padliśmy ofiarą oszustwa, bowiem harmonogram spłaty rat czy wezwania do zapłaty nie trafią na nasz adres. W najgorszym scenariuszu o tym, że jesteśmy dłużnikami, dowiemy się od komornika, który zajmie nam pensję lub przyjdzie do domu zabezpieczyć wartościowe przedmioty* - dodaje **Andrzej Karpiński.**

**Technologia - dobrodziejstwo czy przekleństwo**

Z przygotowywanego na zlecenie ZBP **raportu InfoDok** wynika, że wartość udaremnionych **prób** **wyłudzeń z wykorzystaniem danych osobowych utrzymuje się na poziomie 48 mln złotych kwartalnie**.

Uproszczone procedury w urzędach, bankach czy u notariusza, możliwość załatwienia coraz większej liczby spraw on-line to dobrodziejstwo naszych czasów – usprawnienie obsługi i ułatwienie dla wielu obywateli. W minionym roku podczas rozliczania podatków za 2021 rok aż 19,8 mln deklaracji podatnicy złożyli online. To 91 proc. wszystkich PIT-ów. Na papierze wpłynęło zaledwie 1,9 mln zeznań. Nie inaczej jest w tym roku. **Według informacji Krajowej Administracji Skarbowej**, zaledwie w ciągu trzech pierwszych dni od uruchomienia możliwości składania e-PIT-ów, podatnicy złożyli milion deklaracji.

Bez wątpienia, forma elektroniczna jest najwygodniejszym sposobem rozliczenia PIT. Ten sposób złożenia deklaracji pozwala też oczekiwać szybszego otrzymania zwrotu podatku. Na tym właśnie żerują przestępcy. Podstawiają fałszywy komunikat o mniej lub bardziej spodziewanym zwrocie podatku lub koniecznej dopłacie. Ich próby padają na podatny grunt, szczególnie, gdy adresat działa odruchowo. Dodatkowym wabikiem może być informacja, iż niezwłoczne przekazanie im danych sprawi, że przelew z nadpłatą podatku zostanie zlecony jeszcze dziś.

**Nasze emocje pomagają złodziejom**

Fiskus może przysłać maila z informacją, co i dlaczego powinniśmy zrobić, np. skorygować, dosłać, **ale zalecenia urzędnika należy realizować już na rządowej stronie.** Jednak otrzymując informację, na wszelki wypadek **nie wolno klikać w załączonego w niej linka**, może on bowiem prowadzić do strony łudząco podobnej do rządowej. Nie wolno również otwierać załączników – można w ten sposób zainstalować sobie złośliwe oprogramowanie.

Administracja skarbowa, podobnie jak bank, **nigdy nie żąda podawania danych osobowych poprzez mail czy telefon**. Zasada ta tym bardziej dotyczy loginów czy haseł. Przestępcy jednak wykorzystują socjotechniczne chwyty, abyśmy zapomnieli o tych zasadach.

Technologia umożliwia oszustom podszywanie się pod znane nam numery telefonów urzędów czy instytucji finansowych. Mogą dać się złapać najbardziej zapobiegliwi, którzy pofatygują się, by sprawdzić numer na stronie internetowej urzędu. Pewni, że kontakt pochodzi od zaufanej strony, mogą podać kluczowe dla przestępczej działalności informacje. Z tego powodu najbezpieczniej jest
**nie kontynuować rozmowy, nie korzystać z opcji „oddzwoń” w telefonie, ani nie odpowiadać na SMS-y z linkami.** Należy samemu wykonać połączenie na numer podany na oficjalnej stronie internetowej.

W przypadku kontaktu mailowego, trzeba **sprawdzić nadawcę**. Nie tylko nazwę jaka się wyświetla, ale przede wszystkim adres. Żaden urząd ani poważna instytucja nie wysyła informacji z darmowej skrzynki popularnych dostawców usług mailowych, na pewno też nie będzie się posługiwać domenami zarejestrowanymi w egzotycznych krajach. Np. rządowe adresy kończą się na „gov.pl”. Banki po @ mają najczęściej swoją domenę, czyli adres swojej strony internetowej.

**Dobry patent, by uchronić się przed wyłudzeniem**

Co zrobić by uniknąć wyłudzenia? Wystarczy niewiele, bo raptem osobiste zainteresowanie stanem swojej historii kredytowej. Jednak, by zadziałało w praktyce, niezbędny jest nawyk systematycznego **sprawdzania** [**swojego Raportu BIK**](https://www.bik.pl/klienci-indywidualni/raport-bik). Przejmując nad nim kontrolę, uda się uniknąć zaskoczenia, że pod naszym nazwiskiem widnieje zobowiązanie, o którym nic nie wiemy.

Można też chronić się przed wyłudzeniami na bieżąco, w czym pomagają [**Alerty BIK**](https://www.bik.pl/klienci-indywidualni/alerty-bik)**.** To ostrzeżenia SMS lub e-mail z informacją o tym, że na przykład ktoś nieuprawniony wykorzystuje nasze dane i się pod nas podszywa. Dzięki temu mamy szansę szybko zareagować i powstrzymać oszusta.

*- Automatyczne powiadomienia ostrzegawcze to bardzo wygodne narzędzie prewencyjne, zwłaszcza gdy w grę wchodzi bezpieczeństwo naszych pieniędzy. W czasach gdy większość spraw załatwiamy przez internet, wręcz koniecznością staje się aktywowanie usługi, która niejako czuwa za nas. Alerty BIK działają w czasie rzeczywistym, a powiadomienia przychodzące odzwierciedlają „odpytania” baz BIK lub BIG InfoMonitor składane przez instytucje finansowe. Takie zapytania są standardową procedurą w celu sprawdzenia wiarygodności kredytowej klientów w procesie udzielania kredytów, ale nie tylko. Informacje przekazują, m.in. firmy pożyczkowe przed udzieleniem pożyczki, a także operatorzy telekomunikacyjni, dostawcy gazu czy energii - niemal wszystkie podmioty, które oferując swoje usługi lub udzielając finansowania chcą potwierdzić, że klient będzie im płacić bez opóźnień. Alerty BIK to usługa płatna, może ją mieć każdy, wystarczy ją aktywować w serwisie* [*www.bik.pl*](http://www.bik.pl) *i spać spokojnie* - tłumaczy **Joanna Charlińska, dyrektor ds. sprzedaży detalicznej w BIK**.

**Warto wziąć inicjatywę w swoje ręce. Chodzi przecież o bezpieczeństwo własnych danych
i pieniędzy**. A nawet najlepsze narzędzia informatyczne nie wystarczą, jeżeli sami nie zadbamy o swoje dane i podstawy bezpiecznego zachowania w sieci.

Oczywiście nad systemami bezpieczeństwa czuwają duże instytucje finansowe, np. banki. Beneficjentem zaawansowanych technologii stosowanych w przedsiębiorstwach jesteśmy my wszyscy. Jednak nie zwalnia to z odpowiedzialności samodzielnego nawyku dbania o swoje dane i kontrolowania własnych finansów.

Źródło: Badanie na zlecenie BIK, pt. „Cyberbezpieczeństwo Polaków”, marzec/kwiecień 2023 r., CAWI, Polacy w wieku 18+, N 1057.

**Biuro Informacji Kredytowej S.A.** wspiera bezpieczeństwo instytucji finansowych i ich klientów, udostępniając bezpieczny system wymiany informacji kredytowych i gospodarczych oraz nowatorskie rozwiązania antyfraudowe. Jako jedyne biuro kredytowe w Polsce, 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. Systemowe rozwiązania antyfraudowe w portfolio BIK to: Platforma Antyfraudowa BIK, Platforma Blockchain, Platforma Cyber Fraud Detection oraz nowo budowana Platforma Biometrii Behawioralnej. BIK aktywnie wspiera innowacje, stąd idea powołania piaskownicy technologicznej [BIK HUB](https://www.bikhub.pl/), adresowanej do przedsiębiorców z sektora finansów, a także innych segmentów rynku, startupów, fintechów. 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. 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

kom.: + 48 512 164 131

aleksandra.stankiewicz-billewicz@bik.pl