Materiał\_prasowy\_12.08.2022 r.

**3 popularne cyberoszustwa finansowe, przez które możesz wpaść w długi! Sprawdź, jak się przed nimi ustrzec!**

**Według danych zebranych na zlecenie BIK, aż 84% Polaków obawia się wykorzystania swoich personaliów w wyniku wycieku, a 54% boi się wyłudzenia pieniędzy spowodowanego kradzieżą danych[[1]](#footnote-1). Te obawy są jak najbardziej uzasadnione, szczególnie teraz, gdy trwają wakacje, i gdy cieszymy się beztroskim, zasłużonym wypoczynkiem. Oszuści jednak nie mają urlopu i wciąż szukają coraz to nowych sposobów na to, by zdobyć dostęp do naszych danych… i pieniędzy. I choć mogłoby się wydawać, że nasza świadomość jako użytkowników Internetu – a co za tym idzie, także ostrożność – powinny być coraz większe, to często wystarczy, że cyberprzestępcy nieznacznie zmodyfikują swoje wcześniejsze metody, a kolejne osoby tracą swoje oszczędności albo popadają w długi. Wciąż najczęstszą (i niestety bardzo skuteczną) metodą oszustwa są różne odmiany phisingu, czyli podszywania się pod inną osobę lub instytucję, czego doświadczyło już 34% badanych Polaków[[2]](#footnote-2).To właśnie tę od lat znaną metodę wykorzystał oszust z Rybnika, który zarabiał na swoich ofiarach, „sprzedając” płatny dostęp do stron internetowych oferujących fałszywe pożyczki. Mężczyzna wyłudził łącznie prawie 6 mln zł i oszukał ponad 40 tys. osób![[3]](#footnote-3) Aktualnie często spotykanymi atakami są także te wykorzystujące wizerunek Ministerstwa Finansów czy PGE. Przez brak ostrożności albo niewiedzę możemy w ich wyniku stracić nie tylko bieżące środki z konta, ale i dane, na które przestępcy mogą zaciągnąć kredyt lub pożyczkę w naszym imieniu. Na czym dokładnie polegają popularne w ostatnich miesiącach metody wyłudzeń i jak się przed nimi bronić? O tym w kolejnym materiale Intrum ,,Ogarniam finanse”!**

**Uwaga na fałszywe strony pożyczkowe!**

Trwające wciąż wakacje to czas, gdy wielu szuka dodatkowego źródła finansowania na wymarzony wyjazd. Jednak powinniśmy zachować szczególną ostrożność przed zaciągnięciem szybkiego kredytu, aby opłacić ofertę „last minute”! Oszustom wcale nie trzeba dużo – wystarczy nasze imię, nazwisko i numer PESEL, by mieli możliwość wyłudzenia kredytu. Przestępca po zdobyciu danych zgłasza się do firm pożyczkowych, które udzielają kredytu przy „minimum formalności”. Uproszczona procedura przyznania pożyczki sprawia, że pracownik nie dokonuje dokładnej weryfikacji danych. Niekiedy zdarza się, że informacje w formularzu pożyczkowym pochodzą nawet od trzech różnych osób! Skąd hakerzy biorą dane? Sposobów, jak przestępców – jest wiele.

Najpopularniejszy polega na stworzeniu specjalnej strony internetowej, która do złudzenia przypomina te, które prowadzą przedsiębiorstwa, zajmujące się działalnością pożyczkową. Takie strony zachęcają chwytliwymi sloganami
i bywa, że wykorzystują branding rozpoznawalnych banków czy firm pożyczkowych, przy czym ich „oferta” okazuje się często najbardziej atrakcyjna spośród „konkurencyjnych”. Po wypełnieniu przez ofiarę formularza na stronie, oszuści wysyłają wiadomości mailowe, w których informują o pozytywnym rozpatrzeniu wniosku kredytowego.
W mailu jest informacja o przyznanej pożyczce i link do portalu rzekomo umożliwiającego przelanie pożyczonych pieniędzy bezpośrednio na konto bankowe zainteresowanego. Na takiej stronie po kliknięciu w dowolny przycisk pojawia się jednak komunikat o konieczności pobrania aplikacji na komputer lub telefon w celu uzyskania szczegółów. Są to aplikacje, które umożliwiają zdalne sterowanie i podgląd pulpitu innego urządzenia, z którym aplikacja się łączy. Po instalacji aplikacji oszust ma już wgląd do tego, co wpisujemy w formularzach, może robić zrzuty ekranu
w dowolnym momencie, a nawet nagrywać całą sesję płatności wraz z naszymi widocznymi danymi! Jak obronić się przed takimi działaniami i uchronić nasze pieniądze?

– *Przede wszystkim przed skorzystaniem z jakiejkolwiek oferty kredytu czy pożyczki poza bankiem, należy sprawdzić wszystkie dane adresowe i kontaktowe firmy, która ich udziela. Oszuści w tym wypadku bazują często na tym, że ofiara działa w pośpiechu, poszukując szybkiej, bezproblemowej gotówki. Dlatego często fałszywe strony podają jedynie minimum informacji kontaktowych, jak adres e-mail i ewentualnie numer telefonu. Natomiast legalnie działające i godne zaufania firmy udzielające pożyczek oraz banki są pod tym względem transparentne. Zawsze na ich stronach internetowych możemy sprawdzić dane rejestrowe. Musimy także skrupulatnie zapoznać się z ofertą. Przestępcy nie umieszczają pełnych informacji np. na temat kosztów pożyczki. Próżno szukać też na podejrzanych stronach wzorów umów. Warto też sprawdzić, czy dana firma figuruje w oficjalnych rejestrach, potwierdzających legalną działalność, takich jak: Rejestr Pośredników Kredytowych i Instytucji Pożyczkowych, KRS, czy też Centralna Ewidencja i Informacja o Działalności Gospodarczej. Jest jeszcze „czarna lista”, czyli lista ostrzeżeń publicznych, tworzona przez Komisję Nadzoru Finansowego. Tuz kolei znajdziemy podmioty, które są podejrzane o popełnienie przestępstwa finansowego. Sprawdzenie firmy w tych miejscach nie wymaga dużego wysiłku, bo wszystko możemy zrobić online, a z pewnością taka przezorność bardzo znacząco zminimalizuje ryzyko, że staniemy się ofiarą wyłudzenia danych lub pieniędzy* – radzi **Krzysztof Ekonomiuk, ekspert Intrum.**

Wśród ofert kredytowych naszą szczególną czujność powinny wzbudzić tzw. pożyczki zagraniczne. Scenariusz oszustwa polega tu na tym, że oszuści wysyłają maile z ofertą pożyczki pochodzącej od firmy z zagranicy. W takiej wiadomości gołym okiem widać, że coś jest nie tak. Treść wygląda jak przetłumaczona z translatora i… w istocie, tak jest! Gdy jednak mail trafi do osoby, która nie zwróci uwagi na te szczegóły i podejmie kontakt z ,,firmą”, również dostanie do wypełnienia formularz. W kolejnym kroku oszust prosi o wysłanie skanu naszego dowodu osobistego, ewentualnie przepisanie z niego konkretnych danych w celu weryfikacji naszej osoby albo też o zrobienie niewielkiego „przelewu weryfikacyjnego”, który ma potwierdzić naszą tożsamość. Problem w tym, że również legalnie działające podmioty, podczas przyznawania kredytowania online, stosują takie procedury. Po czym więc poznać oszusta?

– *Przede wszystkim, zwracajmy baczną uwagę na treść wszystkich formularzy i komunikatów, jakie do nas trafiają, zwłaszcza jeśli dotyczą naszych pieniędzy. Jeśli trafimy na jakąś nieścisłość logiczną we wniosku czy błędy językowe, to miejsce, w którym zdecydowanie powinniśmy się wycofać. Nie klikajmy w linki oferujące pożyczkę, rozsyłane mailem czy SMS-em, bo bardzo prawdopodobne, że to próba wyłudzenia „Prawdziwe” banki i instytucje pożyczkowe, nigdy nie poproszą nas też o podanie loginu i hasła do konta, a tym bardziej kodu autoryzacyjnego SMS; nie polecą nam też zainstalowania aplikacji, która pozwoli im wykonywać ruchy na naszym koncie bankowym* – ostrzega **Krzysztof Ekonomiuk, ekspert Intrum.**

**Oszustwa na ankietę Ministerstwa Finansów**

To oszustwo bazuje na wykorzystywaniu autorytetu instytucji oraz na bardzo wiarygodnej (przynajmniej wizualnie) oprawie graficznej. Były już oszustwa na Polski Ład, na Urząd Skarbowy, a niedawno dołączyły do nich wyłudzenia
w oparciu o podszywanie się pod Ministerstwo Finansów. Oszuści wysyłają SMS-y i maile o treści „Akcja Ministerstwa Finansów! Wypełnij krótką ankietę i zyskaj 250 zł na swoje konto.”, wraz z linkiem przenoszącym nas na stronę internetową. Ta wygląda całkiem wiarygodnie. Wspomniana ankieta również nie wzbudza podejrzeń. Kluczem jest uważność na szczegóły. Po dokładnym przejrzeniu strony zorientujemy się, że przycisk służący do przejścia do następnego kroku jest napisany w innym języku. Następnie procedura wygląda dosyć standardowo. Musimy wybrać, do którego banku chcemy dostać obiecane pieniądze. Pojawia się ekran podobny do witryny logowania do naszej bankowości elektronicznej, oszuści liczą, że bez zastanowienia podamy tu swój numer klienta oraz hasło do logowania do banku. Proces kończy to, że na nasz numer telefonu dostajemy kod autoryzacyjny. Jeśli go wpiszemy, to w tym momencie oszust paruje swoją aplikację mobilną z naszym kontemi ma już otwartą drogę do właściwie wszystkich operacji na naszym rachunku: od przeprowadzania transakcji, do zmiany limitów płatności, aż po hasła dostępu.

– *Zanim wypełnimy jakikolwiek formularz, powinniśmy sprawdzić źródło z jakiego pochodzi. W tym wypadku wystarczyłoby wejść na oficjalną stronę Ministerstwa Finansów. Organy państwowe, takie jak MF zawsze oficjalnie informują na stronach internetowych o swoich działaniach, a także przestrzegają tam przed oszustwami. Jeśli jednak mleko już się wylało i nie byliśmy wystarczająco czujni, a oszust posiada już nasze dane do konta bankowego,
w pierwszej kolejności powinniśmy niezwłocznie skontaktować się z naszym bankiem i poinformować o incydencie: zablokować dostęp do karty, zmienić hasła logowania do bankowości internetowej. Należy działać jak najszybciej, bo skradzione w ten sposób pieniądze, bardzo trudno odzyskać, a na zaciągnięcie długów w naszym imieniu wystarczy oszustom w tym wypadku tylko kilka minut* – podpowiada **Krzysztof Ekonomiuk, ekspert Intrum.**

**SMS o odłączeniu energii, czyli oszustwo na PGE**

Przestępcy wykorzystują tu zamieszanie związane z rosnącymi ostatnio w zawrotnym tempie cenami energii, było już kilka fal tego oszustwa. To nic innego jak nowa odsłona kolejnej już wcześniej stosowanej phishingowej metody, wcześniej podszywano się m.in. pod DPD i OLX. Przestępcy szykują na swoje ofiary przynętę w postaci odpowiednio przygotowanych, sfałszowanych e-maili i SMS-ów. Bez problemu wykorzystują także media społecznościowe
i komunikatory i liczą na to, że odbiorca wpadnie w panikę, bo kto z nas nie zainteresowałby się SMS-em o treści „PGE: Na dzień 08.07 zaplanowano odłączenie energii elektrycznej! Prosimy o natychmiastowe uregulowanie należności: LINK”. Brzmi wiarygodnie? Jasne, że tak. Nikt z nas nie chce zostać bez prądu, dlatego ludzie często dają się złapać i bez zastanowienia klikają w złośliwy link. Warto jednak zaznaczyć, że wprawne oko od razu dostrzeże oszustwo. Przede wszystkim należy zwrócić uwagę na treść wiadomości, najczęściej nie posiada ona polskich znaków, a link składa się jedynie z przypadkowych cyfr i liter. Jeśli jednak, będąc w stresie, nie zwrócimy na to uwagi, to jeszcze nic straconego. Link najczęściej przekierowują nas na strony internetowe sfingowane tak, by do złudzenia przypominały oryginalną witrynę PGE. Kluczowe w tym elemencie jest zachowanie spokoju. Metoda na „PGE” działa dosyć standardowo. Tradycyjnie, mamy sfingowany formularz, w którym podajemy swoje dane, bądź ekran logowania do banku, w którym wpisujemy nasz login i hasło, które wędrują wprost do przestępców.

– *W przypadku otrzymania takiej wątpliwej wiadomości, powinniśmy przede wszystkim zachować spokój
i zweryfikować, czy kontakt jest rzetelny. PGE w swojej oficjalnej korespondencji, w której informuje o zaległych płatnościach, bądź* *zamiarze wstrzymania dostaw energii, zawsze podaje numer klienta, numer faktury, termin płatności i kwotę do zapłaty, ale nigdy nie znajdziemy tam linków, które przekierowują bezpośrednio do systemów płatności. Gdy taki otrzymamy, pod żadnym pozorem nie klikajmy w niego, w tym wypadku tylko odpowiednia ostrożność uchroni nasze dane i pieniądze –* wyjaśnia **Krzysztof Ekonomiuk, ekspert Intrum.**

Choć metody przestępców wciąż ewoluują, to najczęściej wykorzystują pewne powtarzalne socjotechniki, przed którymi możemy się skutecznie bronić. Najlepszą bronią jest zawsze weryfikacja i nieuleganie emocjom wszędzie tam, gdzie chodzi o nasze pieniądze.

1. *Cyberbezpieczeństwo Polaków 2022,* badanie przeprowadzone na zlecenie Biura Informacji Kredytowej, przez Quality Watch, 30 marca 2022 r. [↑](#footnote-ref-1)
2. Tamże. [↑](#footnote-ref-2)
3. Źródło: PAP. [↑](#footnote-ref-3)