

Prawie co 4. Polak deklaruje, że w czasie pandemii rozmawiał przez telefon z kimś, kto poprosił go o podanie numeru PESEL, serii dowodu osobistego lub danych do logowania w bankowości elektronicznej. Najczęściej o takie dane pytali „pracownicy banków” i to nie zawsze tych, w którym mamy konto. Równocześnie prawie 20 proc. osób przyznało się, że mogło podać takie informacje osobom trzecim. Najczęściej dotyczyło to osób młodych. Takie wnioski płyną z badania serwisu ChronPESEL.pl i Krajowego Rejestru Długów pod patronatem Urzędu Ochrony Danych Osobowych.

Od kilku tygodni media regularnie ostrzegają przed telefonami od oszustów podszywających się pod pracowników banków lub instytucji finansowych, którzy próbują wyłudzić m.in. dane osobowe oraz informacje potrzebne do logowania w bankowości elektronicznej. Jak wynika z przeprowadzonego badania, z taką sytuacją spotkało się 24 proc. ankietowanych. Najczęściej dotyczyło to mieszkańców małych (do 20 tys.) i średnich miast (20-100 tys. mieszkańców).

Zapytani o to, z kim rozmawiali, ponad połowa (52 proc.) respondentów wskazała na osoby podające się za pracownika banku. Co ciekawe, blisko 18 proc. takich przypadków dotyczyło banku, w którym rozmówca nawet nie miał konta. Dodatkowo prawie co 5. taki telefon był z firmy gazowniczej, energetycznej lub od dostawcy Internetu. O numer PESEL, dane z dowodu osobistego lub hasło do logowania w banku pytali nas również przedstawiciele firm, którzy twierdzili, że wygraliśmy jakiś konkurs (16 proc. wskazań) oraz pracownicy koordynujący bezpłatne badania medyczne (13 proc.). Brak ostrożności w takich sytuacjach może prowadzić do poważnych konsekwencji.

– Takie dane mogą wystarczyć do tego, żeby podrobić nasz dowód osobisty lub zamówić tzw. dowód kolekcjonerski. W ten sposób, korzystając z naszej tożsamości, przestępcy są w stanie zaciągnąć różne zobowiązania finansowe, np. wziąć pożyczkę, podpisać umowę leasingową lub zrobić drogie zakupy na raty, których nie zamierzają potem spłacać. My o wszystkim dowiemy się po czasie z wezwania do zapłaty, które otrzymamy, albo co gorsze po zajęciu konta przez komornika. A trzeba pamiętać że działając w ten sposób sprawni oszuści są w stanie zaciągnąć nawet kilka zobowiązań, z którymi mierzyć się będzie musiała ich ofiara – ostrzega Bartłomiej Drozd, ekspert serwisu ChronPESEL.pl.

Młodzi ludzie częściej przekazują swoje dane

W obliczu powszechnego dostępu do wiadomości, zwłaszcza w Internecie, wydawać by się mogło, że ludzie będą do takich telefonów podchodzić ostrożnie. Tymczasem nawet co 5. ankietowany (18,4 proc.) przyznał się do tego, że mogło mu się zdarzyć przekazać dane do logowania osobom trzecim. Wprost deklaruje to 11 proc. badanych, pozostali nie mają pewności. Co zastanawiające, najczęściej dotyczyło to osób młodych w wieku między 18 a 24 rokiem życia (29 proc. w tej grupie). Wraz z wiekiem ta tendencja spada. Najrzadziej dane do logowania przekazują respondenci w najstarszych grupach wiekowych.

Takie podejście wykorzystują oszuści podszywający się pod bank lub inną instytucję finansową, którzy dzwoniąc przedstawiają się jako konsultant albo opiekun klienta i informują swoich rozmówców, że ktoś próbował zaciągnąć zobowiązanie na ich dane lub chcą zweryfikować jakieś podejrzaną transakcję. W ten sposób wywołują u potencjalnej ofiary poczucie zagrożenia, dzięki czemu, gdy chwilę później oferują pomoc sprawiają wrażenie bardzo wiarygodnych. Oszustwo polega na tym, że pod pozorem potwierdzenia tożsamości klienta proszą go o podanie wszystkich danych potrzebnych do zalogowania łącznie z hasłem do bankowości elektronicznej.

– W takich sytuacjach warto zachować zimną krew. Przede wszystkim musimy wiedzieć, że pracownicy banku nie będą pytali nas o numery dokumentów czy dane do logowania. Sama taka prośba powinna

wzbudzić nasze wątpliwości. Dlatego najlepiej zawsze samemu zadzwonić do swojego banku i zapytać, czy rzeczywiście mamy powody do niepokoju. Jeśli nie, powinniśmy poinformować instytucję o tym, że ktoś się pod nią podszywa i dzwoni do klientów próbując ich oszukać. Sprawę powinniśmy też zgłosić na policję, ponieważ może to świadczyć o tym, że ktoś gdzieś wyłudził nasze dane osobowe. Warto sprawdzić również w biurze informacji gospodarczej, czy ktoś nie próbował już wykorzystać naszego numeru PESEL – tłumaczy Bartłomiej Drozd.

Młódzież stawia wszystko na jedno hasło

Brak ostrożności w przekazywaniu danych do logowania jest niepokojący również z innego powodu. W przeprowadzonym badaniu aż 36,5 proc. ankietowanych zadeklarowało, że używa tego samego hasła do logowania w kilku serwisach. To oznacza, że wystarczy je raz zdobyć, żeby całkowicie legalnie załogować się na kilku naszych kontach. Najmniejszą ostrożność w tym aspekcie znów wykazują ludzie młodzi, w wieku między 18 a 24 rokiem życia. Nawet połowa z nich (50 proc.) loguje się do kilku serwisów korzystając z tego samego hasła.

– W takim wypadku nie uratuje nas nawet odpowiednio trudne i skomplikowane hasło. Dlatego w każdym serwisie powinniśmy się logować w inny sposób. Dzięki temu zwiększymy swoje bezpieczeństwo. Dodatkowo w sytuacji, w której mamy chociaż cień podejrzenia, że ktoś zdobył nasze hasło, powinniśmy je natychmiast zmienić – dodaje Bartłomiej Drozd.

Warto korzystać także z logowania dwuskładnikowego. Jak wynika z przeprowadzonego badania, 35,5 proc. ankietowanych uważa, że logując się do bankowości elektronicznej oprócz wpisywania hasła najbezpieczniej będzie potwierdzić to za pomocą kodu SMS. Dla 25 proc. taką gwarancją jest z kolei weryfikacja linii papilarnych a dla prawie 10 proc. weryfikacja twarzy. Świadczy to również o tym, że podstawowym narzędziem do korzystania z bankowości elektronicznej jest nasz telefon komórkowy.

Źródło: IP