fundacja instytut
CYBERBEZPIECZEŃSTWA

Przekręt nigeryjski

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

Witam! Jestem Książę Ahmed, członek królewskiej rodziny z Arabii Saudyjskiej. Piszę do Pani z poważną i pilną prośbą. Ze względu na obecną niestabilną sytuację polityczną w naszym kraju zostałem zmuszony do wyprowadzenia znacznych środków finansowych z Arabii Saudyjskiej. Kwota ta wynosi 50 milionów dolarów i obecnie jest zdeponowana na koncie w jednym z szwajcarskich banków. Ze względu na moją sytuację nie mogę sam zarządzać tymi środkami, dlatego proszę o pomoc w transferze tych pieniędzy na Pani konto bankowe. Oferuję 20% kwoty jako wynagrodzenie za pomoc. Jednakże, aby zrealizować ten transfer, muszę uiścić pewne opłaty administracyjne oraz bankowe w wysokości 500 dolarów, a nie mam aktualnie dostępu do swoich środków. W związku z tym proszę o pomoc w opłaceniu tych niezbędnych kosztów, które zostaną zwrócone wraz z wynagrodzeniem po zakończeniu naszej współpracy. W odpowiedzi na wiadomość proszę podać również Pani dane, takie jak: pełne imię i nazwisko, pesel, adres, numer konta bankowego, które są niezbędne do zgłoszenia przeze mnie planowanych operacji.

Z wyrazami szacunku

Książę Ahmed

Brzmi dość podejrzanie, prawda? Powyższa treść to przykład przekrętu nigeryjskiego. Może wydawać się to mało prawdopodobne, jednak na całym świecie wciąż są osoby, które padają ofiarą tego rodzaju cyberprzestępstwa, w efekcie tracąc najczęściej bezpowrotnie swoje pieniądze.

Czym jest przekręt nigeryjski?

Przekręt nigeryjski (zwany także fraudem nigeryjskim lub szwindlem nigeryjskim) to pewien rodzaj spamu – oszustwo nastawione zawsze na zysk finansowy. Potencjalne ofiary otrzymują go na swoją skrzynkę mailową. Autorzy takich nieprawdziwych wiadomości najczęściej dokonują wyboru adresatów zupełnie przypadkowo. Dać się oszukać na maila podobnego do przedstawionego powyżej wydaje się równie niemoż-

liwe, jak realne zaistnienie takiej sytuacji w Arabii Saudyjskiej. Cyberprzestępcy najczęściej jednak nie poprzestają na jednym mailu i usiłują wciągnąć ofiarę w pewną grę psychologiczną. Pierwsza wiadomość z reguły informuje o możliwości znacznego wzbogacenia się. Zdarza się, że jest w niej opisana także nagła i tragiczna sytuacja, w jakiej znalazł się autor (zależnie od wariantu przekrętu, o tym w dalszej części artykułu). Jeśli adresat takiego maila odpowie na wiadomość, przestępca usilnie zachęca do wpłacenia kwot pozornie niewielkich w stosunku do obiecanego zarobku. Zdarza się, że oszuści swoje słowa potwierdzają zdjęciami lub dokumentacją np. z banku. Oczywiście rzekome dowody są spreparowane lub stanowią efekt pracy sztucznej inteligencji. Po pierwszej wpłacie cyberprzestępcy przyjmują różne strategie dalszego prowadzenia konwersacji z ofiarą. Jedni namawiają na wpłatę wielu małych sum, inni po kilku drobnych datkach wymuszają przelanie znacznej sumy pieniędzy, a kolejni wyłudzają dane i włamują się na konto bankowe ofiary, sami biorąc to, co i tak planują zabrać.

Warianty przekrętu nigeryjskiego

Tak jak na przedstawionym przykładzie (wymyślonym na potrzeby artykułu), przekręt może przybrać formę prośby o pomoc w transferze pieniędzy z zagranicznych kont. Oszuści podszywają się pod bogate osoby, jak np. członkowie królewskich rodzin, biznesmeni czy wysocy urzędnicy, którzy rzekomo mają trudności z dostępem do swoich funduszy z powodu sytuacji politycznej, prawnej, rodzinnej itp. W zamian za pomoc w tym transferze obiecują ofiarom znaczne wynagrodzenie, często wynoszące miliony dolarów, których rzecz jasna ofiara nigdy nie zobaczy. Kolejnym wariantem jest wizja możliwości otrzymania spadku. Nie wierz w to, że twoja rodzina z drugiego końca świata, o której istnieniu nie wiedziałeś, pozostawiła dla ciebie pałac i milion dolarów, jeśli tylko opłacisz czynności administracyjne związane z testamentem. Przekręt nigeryjski może również przybierać formę prośby o pomoc w opłaceniu leczenia chorego członka rodziny. W tym wariancie oszuści kontaktują się z ofiarami i opisują dramatyczną sytuację, w której znajduje się ich bliski krewny, pilnie potrzebujący kosztownego leczenia. Historia ma na celu wzbudzenie współczucia i przeświadczenia o pilności tej sprawy, aby ofiara jak najszybciej przelała środki. To tylko wybrane przykłady wariantów przekrętu. Wyobraźnia cyberprzestępców nie zna granic, a metody wyłudzeń wciąż ewoluują i są coraz bardziej udoskonalane.

Oszustwo starsze niż Internet

Pierwsze oszustwa tego typu notowane były już na przełomie XVIII i XIX wieku, kiedy popularnością cieszył się przekręt na hiszpańskiego więźnia. Oszust usiłował wmówić potencjalnej ofierze, że jest w kontakcie z zamożną osobą, niesłusznie osadzoną w hiszpańskim więzieniu. W zamian za datki na zorganizowanie ucieczki oferowano znacznie wyższą kwotę, która miała zostać wypłacona, gdy więzień będzie już na wolności. Przekręt ten odbywał się za pomocą tradycyjnych listów lub bezpośrednich próśb. Po przekazaniu umówionej sumy oszust znikał bez śladu, podobnie jak ma to miejsce dziś. W związku z dużym postępem technologicznym z czasem zaczęto korzystać z faxu, telefonu, a wreszcie z poczty elektronicznej, co w porównaniu z analogowymi listami zwiększyło zasięgi wpływu oszustów. Obecnie technologia jest na tyle zaawansowana, że maile tego typu może tworzyć i wysyłać bot, który pracując całodobowo, osiąga liczbę nawet kilku tysięcy wysłanych wiadomości na godzinę. Statystycznie na 500 takich maili odpowiedzi doczeka się 7.

Nazwa przekrętu

Wbrew pozorom Nigeria nie jest wcale państwem, skąd wysyła się najwięcej tego typu wiadomości. Przekręt nigeryjski to już zjawisko globalne. Ten afrykański kraj jest jednak często wymieniany w mailach jako np. miejsce zamieszkania nadawcy. Inna nazwa tego cyberprzestępstwa to 419 scam, co ma swoje źródło w numerze artykułu w nigeryjskim kodeksie karnym, który daje podstawę do ścigania takich procederów.

Jak się chronić?

Nie ma na to pytanie prostszej odpowiedzi niż zachowanie czujności i zasady ograniczonego zaufania do wiadomości, zwłaszcza otrzymywanych z obcych adresów mailowych. Nasze podejrzenia powinna wzbudzić nie tylko treść, lecz także literówki oraz błędy składniowe i ortograficzne. Oszuści starają się dopasować język maila do tego, którym posługuje się potencjalna ofiara, jednak nie zawsze ich tłumaczenia są perfekcyjne. Na wiadomości dotyczące szybkiego przekazania niebotycznej fortuny po prostu nie reagujmy. Edukujmy się i stale podnośmy nasz poziom wiedzy o cyberbezpieczeństwie i najnowszych technikach oszukiwania internautów, by nie dać się nabrać na dynamicznie zmieniające się metody działań przestępców. Jeśli jednak ty lub ktoś z twojego otoczenia dał się oszukać na przekręt nigeryjski, sprawę natychmiast należy zgłosić na policję. Nie usuwaj konwersacji z oszustem. Zachowaj ją na potrzeby środków dowodowych. Skontaktuj się także niezwłocznie ze swoim bankiem z celu zablokowania dostępnych na koncie środków finansowych.

Nadal nie wierzę, że ktoś może się na to nabrać...

Odzyskanie pieniędzy po przekazaniu ich oszustowi może okazać bardzo się trudne, a proces działania służb – długotrwały. W przypadku gdy ofiara zorientuje się w sytuacji po przekazaniu nieznacznych kwot, zazwyczaj nie nagłaśnia sprawy i nie dochodzi swoich racji na drodze sądowej. Są jednak sytuacje, kiedy socjotechnika oszustów jest tak zaawansowana, że zmanipulowane ofiary tracą oszczędności swojego życia. Na początku 2024 roku 41-letnia mieszkanka powiatu lęborskiego została oszukana przez rzekomego amerykańskiego żołnierza. Kobieta korespondowała z nim ponad rok, aż ten poprosił ją o znaczną sumę pieniędzy, które miał oddać, gdy przyjedzie do Polski, by oświadczyć się swojej internetowej miłości. Aby wspomóc przyszłego narzeczonego, kobieta zaciągnęła pożyczki w kilku bankach na łączną sumę 220 000 złotych. Jej całość przelała na konto oszusta, który po otrzymaniu pieniędzy zerwał kontakt. Rok wcześniej swoje pieniądze straciła mieszkanka Sądecczyzny, której obiecano ćwierć miliona euro spadku. Za pośrednictwem mediów społecznościowych skontaktowała się z nią osoba z innego kraju, twierdząc, że posiada wielki majątek i nie ma żadnego spadkobiercy, któremu może go pozostawić. Z tego powodu chce podzielić się fortuną z internautką. Aby otrzymać pieniądze, ofiara musiała jedynie zapłacić 4 500 złotych, by pokryć z tych pieniędzy załatwianie formalności administracyjnych, co w stosunku do 25 000 euro zysku nie wydawało się tak wielką sumą. Po przekazaniu kwoty zamożny znajomy bezpowrotnie zniknął. Przykłady udanych manipulacji można mnożyć, niestety niewiele jest sytuacji, kiedy udało się namierzyć oszusta i odzyskać wyłudzoną kwotę.

Źródła:

Maciejewski K., „Amerykański żołnierz” oszukał 41-latkę na 220 tys. zł, forsal.pl, 22.03.2024 r., https://forsal.pl/finanse/finanse-osobiste/artykuly/9469639,amerykanski-zolnierz-oszukal-41-latke-na-220-tys-zl.html.

Miała otrzymać w spadku ćwierć miliona euro. Straciła swoje oszczędności, policja.pl, 1.02.2023 r., https://www.policja.pl/pol/aktualnosci/227760,Miala-otrzymac-w-spadku-cwierc-miliona-euro-Stracila-swoje-oszczednosci.html.

Nigeryjski przekręt, CERT Polska, 24.02.2023 r., https://cert.pl/posts/2023/02/nigerian-scam/.

Nigeryjski przekręt? Oto oszustwo starsze niż Internet!, YouTube, 23.09.2020 r., https://www.youtube.com/watch?v=Vd1sG9MY4is.

Nigeryjski szwindel, Wikipedia, https://pl.wikipedia.org/wiki/Nigeryjski_szwindel.

fundacja instytut CYBERBEZPIECZEŃSTWA

www.instytutcyber.pl

Fundusz Sprawiedliwości Ministerstwo Sprawiedliwości

Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości