ŻYJ BEZPIECZNIE

Źródło: http://zyjbezpiecznie.policja.pl/zb/komputer-i-internet/47346,quotNigeryjski-szwindelquot.html
Wygenerowano: Wtorek, 23 stycznia 2018, 19:00

"NIGERYJSKI SZWINDEL"

Zwykle zaczyna się podobnie. Autor przesłanego do nas maila informuje, że możemy otrzymać olbrzymie pieniądze, a fortuna jest dosłownie na wyciągnięcie ręki. Musimy tylko dopełnić kilku formalności i dokonać opłat manipulacyjnych. Te kwoty, w porównaniu z gotówką, jaką mamy dostać, wydają się jednak niewielkie. Dopiero po jakimś czasie okazuje się, że nie czeka na nas żaden spadek ani wygrana, ale padliśmy ofiarą oszustów.

"Oszustwo nigeryjskie" lub "nigeryjski szwindel" – tym terminem policjanci określają specyficzny i stosunkowo nowy rodzaj oszustw. Ten przestępczy proceder najczęściej rozpoczyna się od kontaktu, który przestępcy nawiązują z pokrzywdzonymi za pośrednictwem poczty elektronicznej. Polega on na wciągnięciu ofiary w grę psychologiczną. Jej fabuła oparta jest na fikcyjnym transferze dużej kwoty pieniędzy z jednego z krajów afrykańskich, zwykle Nigerii. W rzeczywistości chodzi po prostu o wyłudzenie od ofiar pieniędzy dzięki wykorzystaniu wymyślonej historii. Ofiarami wcześniej padali przypadkowi właściciele skrzynek mailowych. Teraz coraz częściej przestępcy starannie dobierają tych, których chcą oszukać.

Na arenie międzynarodowej przypadki takie bada U. S. Secret Service, ale nawet ta służba stoi na stanowisku, że odzyskanie pieniędzy utraconych w wyniku „oszustwa nigeryjskiego" jest praktycznie niemożliwe. Aby móc skutecznie bronić się przed oszustami warto wiedzieć, jakimi metodami się oni posługują.

"Na uchodźcę politycznego z czarnego lądu"

Przestępca kontaktuje się z ofiarą najczęściej wykorzystując do tego pocztę elektroniczną, rzadziej telefon. W korespondencji pada propozycja otrzymania ogromniej kwoty pieniędzy. Chodzi o części fortuny, jaką oszust posiada (odziedziczył), ale której sam nie może podjąć z banku z różnych przyczyn. Niekiedy oszust podaje się za uchodźcę politycznego, dziedzica fortuny zgromadzonej przez jednego z przywódców któregoś z państw afrykańskich obalonego w trakcie przewrotu politycznego. Chodzi zwykle o bardzo duże sumy, 20 – 30 mln USD, a oszust w zamian za pomoc w jej odzyskaniu oferuje nawet połowę tej kwoty.

„Pomoc" ta wymaga jednak od ofiary finansowania kolejnych kroków, jakie oszust musi czynić by sfinalizować przelew majątku na konto wskazane przez ofiarę. W cyklicznie otrzymywanej korespondencji ofiara dowiaduje się, że oszust musi np. zarejestrować działalność gospodarczą, posłużyć się kilkoma łapówkami by przekupić bankierów, skorumpowanych policjantów lub innych urzędników państwowych w jego kraju lub musi opłacić procedurę wystawienia certyfikatów przez bank, poświadczających, że pieniądze nie pochodzą z nielegalnego źródła (np. z działalności terrorystycznej lub handlu narkotykami). Ofiara, która już widzi siebie jako milionera, pokrywa kolejne koszty związane z finalizacją całej operacji. Pieniądze przejmuje oszust, który od czasu do czasu uwiarygodnia historię przesyłając pocztą elektroniczną spreparowane certyfikaty, kopie potwierdzeń przelewów, itp. W tym momencie rozpoczyna się gra, która ma na celu jak najdłuższe zwodzenie ofiary i wyłudzenie jak największej ilości pieniędzy. Zazwyczaj ofiara na tym etapie zaczyna podejrzewać oszustwo i w pewnym momencie przestaje płacić. Oszust jednak osiągnął zamierzony cel – praktycznie już po otrzymaniu pierwszej wpłaty. Gdy ofiara przerywa „finansowanie operacji" często dochodzi do gróźb lub zmiany fabuły gry. Oszust teraz może podawać się za inną osobę, ale są to tylko próby wyłudzenia kolejnych sum.

Na "inwestora"

Przestępca kontaktuje się z ofiarą najczęściej wykorzystując do tego wyłącznie pocztę elektroniczną. Oszust podaje się za młodego, wykształconego człowieka, któremu udało się „wybić" w jego rodzinnym kraju (młody prawnik, student, modelka). Jego ojciec lub przyjaciel posiada ogromny majątek, który chce korzystnie zainwestować. Ofiara ma pomóc w inwestowaniu pieniędzy w swoim rodzimym kraju. Dalszy ciąg jest analogiczny do poprzedniej metody.

Na "wygraną na loterii"

Potencjalna ofiara otrzymuje pocztą elektroniczną spreparowaną wiadomość o wygranej dużej sumy pieniędzy w jednej z (narodowych) loterii jakiegoś europejskiego kraju. Ostatnio oszuści najczęściej podszywali się pod organizatorów loterii hiszpańskich. Wraz z informacją otrzymujemy certyfikat uprawdopodobniający wygraną oraz istnienie samej loterii. Kwoty, jakie mamy otrzymać są zwykle znacznie niższe niż w klasycznym „oszustwie nigeryjskim", Oszust, by rozwiać wszelkie podejrzenia ofiary, twierdzi, że nagrodę można odebrać osobiście, podając dokładny adres i telefony kontaktowe. Mało kto jednak decyduje się na precyzyjne sprawdzenie tych danych. Zwykle pokrzywdzeni deklarują, że chcą otrzymać wygraną w formie międzynarodowego przelewu bankowego. Tu pojawiają się pierwsze opłaty, które ofiara zobowiązana jest uiścić by móc odebrać nagrodę – opłata dla prawnika, opłata za wystawienie kilku nieznanego pochodzenia wewnętrznych dokumentów banku i certyfikatów, do opłacenia podatku od wzbogacenia włącznie. Jak w każdym z omawianych przypadków żadna wygrana nie istnieje, a oszust podtrzymuje kontakt tak długo, jak długo ofiara dokonuje kolejnych wpłat. Niekiedy ofiara informuje, że posiada połowę żądanej przez oszusta kwoty, na co oszust odpowiada, że drugą część pokryje on ze środków własnych, które później ofiara mu zwróci. Wszystko ma służyć temu, by nie wstrzymywać całej procedury. Wreszcie oszust wysyła pocztą tradycyjną, nie tylko elektroniczną, kolorowe certyfikaty i potwierdzenia przyjęcia przez różne instytucje i banki opłat od ofiary. Zaś pieniądze z wygranej giną gdzieś na „czarnym lądzie"…

Na "konta w banku bez właściciela"

Przestępca, udając najczęściej pracownika banku, kontaktuje się z ofiarą za pośrednictwem poczty elektronicznej. Potencjalna ofiara jest informowana, że klient banku zmarł lub zginął w tragicznym wypadku i zostawił po sobie konto z ogromną sumą pieniędzy. Nie wskazał jednocześnie żadnych spadkobierców, a bank nie mógł ustalić żadnego członka jego rodziny. Po odczekaniu kilku lub nawet kilkunastu lat bank zamierza zlikwidować martwe konto i szuka kogoś, kto przejmie jego zawartość.

Kiedy ofiara wyrazi zainteresowanie, oszust przysyła wiadomość ze szczegółami historii. Często załącza dokumenty (wątpliwej jakości) potwierdzające istnienie przedmiotowego konta, należącego do zmarłego milionera. Czasami oszuści decydują się również na kontakt telefoniczny. Z ofiarą kontaktują się kolejne osoby - dyrektor banku, prawnik lub inny urzędnik, który jest władny wystawiać lub uwiarygodniać dokumenty - które mają uwiarygodnić całą historię. Wtedy też pojawiają się pierwsze informacje, że ofiara będzie musiała sfinansować kilka przedsięwzięć, by w końcu móc cieszyć się milionami. Okazuje się, że ma ponieść opłaty za wystawienie przez bank lub inne urzędy certyfikatów, poświadczających, że pieniądze pochodzą z legalnego źródła, za usługi prawników oraz koszty operacyjne w banku. Oszust podtrzymuje korespondencję prosząc o kolejne wpłaty tak długo jak na to pozwala naiwność ofiary oszustwa.

Pozostawione miliony na koncie są oczywiście fikcją, jak również to, że informacja pochodzi z banku. Nazwiska pracowników banku mogą być prawdziwe, gdyż przeważnie są to dane ogólnie dostępne w Internecie. Należy jednak zwrócić uwagę na numery telefonów, których nie znajdziemy w informacjach kontaktowych rzeczywiście istniejącego banku, a adresy e-mail używane przez oszustów często należą do puli adresów serwerów oferujących bezpłatną rejestrację konta poczty elektronicznej, (np. Yahoo, Google Gmail).

Na "aukcje internetową"

Ofiara jest wyszukiwana na portalu aukcyjnym, gdzie wystawia jakiś wartościowy sprzęt elektroniczny, np. laptop lub sprzęt fotograficzny. Kontakt za pośrednictwem poczty elektronicznej nawiązuje oszust, który sprawia wrażenie bardzo zainteresowanego zakupem oferowanego towaru. Wartościowy przedmiot ma najczęściej stanowić prezent dla bliskiej osoby, przebywającej w innym kraju niż oszust. Oszustowi bardzo zależy na czasie wysyłki, który ma być jak najkrótszy, więc sprzedaż musi się odbyć poza aukcją, jeżeli aukcji nie można zakończyć z opcją „kup teraz". Oszust takie niedogodności jest gotów wynagrodzić oferując nawet dwukrotnie wyższą kwotę niż żąda sprzedający.

Wielu sprzedających zgadza się wysłać towar, oczywiście po otrzymaniu zapłaty. Tu pojawia się charakterystyczny dla tego oszustwa sposób działania sprawcy. Po zakończeniu transakcji, najczęściej drogą elektroniczną, ofiara otrzymuje spreparowany skan potwierdzenia dokonania wpłaty pieniędzy, wraz z komentarzem, iż przelew pieniędzy z Afryki trwa kilka dni, a prezent musi być dostarczony niezwłocznie. Często wpłata ma odbywać się za pośrednictwem takich systemów płatności, jak Bidpay, Money Gram, Western Union. Oszust prosi, by ofiara wysłała towar przed otrzymaniem wpłaty na konto.

Ma przecież potwierdzenie dokonania wpłaty w postaci zeskanowanego dokumentu. Zazwyczaj sprzedający godzi się na to. Jeżeli natomiast nie wyraża zgody, jest straszony złamaniem umowy, oskarżany o oszustwo, a w skrajnych przypadkach straszony nawet zgłoszeniem sprawy do Interpolu. W konsekwencji sprzedający wysyła towar, ale nigdy nie otrzymuje za niego pieniędzy.

Na "spadek"

Pierwszy kontakt z wytypowaną ofiarą ma wyglądać na zupełnie przypadkowy. Może to być „przypadkowe" spotkanie z osobą, która twierdzi, że nosi takie same nazwisko jak ofiara (bądź nazwisko panieńskie matki ofiary), lub zna kogoś kto mógł należeć do rodziny ofiary. Scenariuszy może być wiele. Chodzi tylko o to, by w pamięci ofiary utkwił fakt, że gdzieś za granicą żyje ktoś, kto należy do jej rodziny, wie o istnieniu ofiary, mimo że nie utrzymuje stałego kontaktu. Przestępcy śledzą wszystkie informacje, które mogą świadczyć o nagłej śmierci (katastrofa komunikacyjna, pożar lub trzęsienie ziemi) osoby o takim samym nazwisku jak potencjalna ofiara. Następnie kontaktują się z ofiarą najczęściej wykorzystując do tego pocztę elektroniczną, rzadziej telefon. W korespondencji informują potencjalną ofiarę, że jest jedynym żyjącym spadkobiercą dalekiego krewnego, który niedawno stracił życie, np. w katastrofie lotniczej (dane najczęściej są ogólnie dostępne w Internecie) i nie pozostawił potomstwa, a w testamencie swój ogromny majątek postanowił przekazać jedynemu znanemu krewnemu, czyli wytypowanej potencjalnej ofierze oszustwa. Odziedziczoną fortunę ofiara może podjąć z banku po dopełnieniu kilku formalności i opłaceniu należności. Ofiara ,na polecenie oszusta podającego się za prawnika bądź bankiera, zaczyna finansować kolejne wydatki. Jak w przypadku innych oszustw nigeryjskich, oszuści uwiarygodniają całą historię przesyłając pocztą elektroniczną spreparowane certyfikaty, kopie potwierdzeń przelewów, itp. Również w tym przypadku, rozpoczyna się gra na zwłokę, która ma na celu jak najdłuższe zwodzenie ofiary i wyłudzenie jak największej kwoty pieniędzy.

By nie paść ofiarą oszustwa zachowajmy rozwagę i rozsądek!

Pamiętajmy:

1. Jeżeli zostaliśmy wybrani na pomocnika w odzyskaniu pieniędzy przez uchodźcę politycznego z czarnego lądu i za to mamy otrzymać np. 12 milionów dolarów, możemy być pewni, że jest to oszustwo.

2. Jeżeli otrzymamy e-mail z informacją, że zostaliśmy zwycięzcami zagranicznej loterii, w której nie braliśmy udziału, to śmiało możemy potraktować tą informację jako spam i od razu przekierować ją do kosza.

3. Jeżeli otrzymamy niespodziewanie miliony dolarów w spadku po krewnym, o którego istnieniu nie mieliśmy pojęcia, a warunkiem otrzymania fortuny jest dokonanie określonych wpłat, możemy być niemal pewni, że ktoś próbuje nas oszukać,

4. Uważajmy, jeżeli ktoś za przekazanie nam ogromnej kwoty pieniędzy żąda opłat manipulacyjnych (opłacania prawników, certyfikatów),

5. Pamiętajmy, że certyfikaty wystawiane przez różne instytucje, to dokumenty, które tak jak dokumenty identyfikacyjne, papiery wartościowe i banknoty, mają odpowiednie zabezpieczenia - hologramy, recto-verso, czy mikrodruk, które po wykonaniu skanowania (digitalizacji obrazu), tracą swoje właściwości, a tym samym przesłany nam skan certyfikatu nie ma żadnej wartości i wagi prawnej.

6. Po zakończeniu transakcji z opcją „wpłata na konto bankowe" należy trzymać się sztywno podstawowej zasady – towar wysyła się wyłącznie dopiero po zaksięgowaniu pełnej kwoty na koncie bankowym.

Materiały: Biuro Kryminalne KGP (Jak uniknąć "oszustwa nigeryjskiego" - http://www.policja.pl/portal/pol/154/39219/Jak_uniknac_quotoszustwa_nigeryjskiegoquot.html)

Ocena: 3.6/5 (10)

Tweetnij

komputery oszustwa internet