ZWIĄZEK BANKÓW POLSKICH

Komunikat
FinCERT.pl – Bankowego Centrum Cyberbezpieczeństwa ZBP
z dnia 21 lutego 2022 r.
w sprawie podszywania się oszustów pod instytucje zaufania publicznego
w kontaktach z osobami duchownymi

Wyłudzanie pieniędzy poprzez udawanie policjanta, prokuratora, innego urzędnika instytucji państwowej lub pracownika banku od lat zbiera żniwa. W ostatnich kilku tygodniach FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa Związku Banków Polskich oraz organy i instytucje, z którymi FinCERT.pl - BCC ZBP współpracuje otrzymują coraz więcej sygnałów o oszustwach i próbach oszustw dokonywanych na przedstawicielach Kościoła.

Niepokojące sygnały docierają z całej Polski i dotyczą osób w różnym wieku, które ufając rozmówcy w dobrej wierze przekazują środki finansowe z kont parafii, zakonów lub kont prywatnych osób duchownych.

Schemat działania przestępców może być różny, ale cechą charakterystyczną jest to, że podczas rozmowy telefonicznej:

1) **oszust podszywa się pod osobę** działającą z ramienia instytucji zaufania publicznego np. policjanta, inspektora urzędu skarbowego, prokuratora, pracownika banku itp. Uwaga: na urządzeniu ofiary może wyświetlić się oficjalny numer telefonu przypisany do danej instytucji;

2) **żąda lub intensywnie nalega na przekazanie** pieniędzy, numerów pin, kodów autoryzacyjnych, danych poufnych służących do logowania do bankowości internetowej, kodów służących do dodania urządzenia zaufanego lub nakłania ofiarę do zainstalowania aplikacji dającej przestępcom zdalny dostęp do komputera ofiary;

3) **swoje żądanie oszust uwiarygadnia odpowiednią historią** np. udziałem w tajnej akcji związanej z rozbiciem grupy przestępczej, zagrożeniem związanym z kradzieżą środków z konta bankowego itp.; ulegając presji atakowane w ten sposób osoby „dobrowolnie" dokonują przelewu środków np. na rzekome operacyjne konta Policji lub udostępniają dane, które oszustom służą do logowania do usług bankowości internetowej i mobilnej, aby przejąć środki osób pokrzywdzonych.

Powyżej opisany sposób działania jest najczęściej spotykanym w ostatnim okresie. Jednak grupy przestępcze zmieniają schemat postępowania i poza wyżej wymienionymi elementami mogą pojawić się inne np. kontakt „doradcy finansowego", który w trudnych czasach pomoże zainwestować środki w giełdę kryptowalut lub „pracownika banku", który zaproponuje „LOKATĘ NA PREFERENCYJNYCH

WARUNKACH” (założenie takiej lokaty będzie odbiegało od procedur stosowanych w banku obsługującym parafię).

Scenariuszy jest znacznie więcej, a wszystkie one mają na celu wpłynięcie na emocje rozmówcy w taki sposób, aby jego troska, zaniepokojenie czy poczucie obowiązku doprowadziły do wykonania przelewu, przekazania poufnych danych, przy pomocy których oszuści wyprowadzą środki z rachunku bankowego lub odbiorą gotówkę.

Jak się chronić?

Należy stosować się do kilku ważnych zasad:

1) nigdy nie ujawniać kodów do bankowości internetowej oraz kodów 3D Secure wykorzystywanych do autoryzacji transakcji kartowych w Internecie, przychodzących na telefon;
2) zawsze należy czytać treść SMS-ów jakie przychodzą na telefon lub komunikatów w aplikacji mobilnej w trakcie połączenia z rzekomym policjantem, urzędnikiem itp. (z ich treści może wynikać, że akceptuje się transakcję, którą przygotowali przestępcy);
3) jeżeli rozmowa wzbudza jakiekolwiek wątpliwości lub niepokój, należy rozłączyć się, odczekać minimum 30 sekund, a następnie samodzielnie połączyć z instytucją, z której telefonował rzekomy przedstawiciel (w takim przypadku koniecznie należy wybrać oficjalny numer na klawiaturze numerycznej zamiast oddzwaniać na wcześniejsze połączenie);
4) zachować zdrowy rozsądek i zimną krew, nawet jeżeli zostało się poinformowanym o potencjalnym zagrożeniu np. o utracie środków; należy ze spokojem zastanowić się, czy środki naprawdę mogą być zagrożone, czy może rozmowa prowadzona jest z oszustem, który chce wykorzystać sytuację i skłonić nas do pochopnej decyzji; dobrym krokiem będzie przerwanie połączenia i ponowne jego zainicjowanie zgodnie z zasadą powyżej;
5) należy zawsze mieć świadomość, że wyświetlony numer telefonu lub nazwa banku nie są gwarancją, że rozmawiamy z prawdziwym urzędnikiem; dlatego nie należy podawać żadnych informacji poufnych, w szczególności w sytuacji, kiedy kontakt jest inicjowany z zewnątrz, a nie przez nas samych.

W przypadku podejrzenia próby popełnienia przestępstwa lub gdy przestępstwo to zostało popełnione należy niezwłocznie poinformować o tym fakcie swój bank oraz złożyć stosowne zawiadomienie na Policję lub do Prokuratury. Szybkość złożenia takiego zawiadomienia może zwiększyć szansę uratowania utraconych środków, które fizycznie mogły jeszcze nie zostać wypłacone przez oszustów.

FinCERT.pl - Bankowe Centrum Cyberbezpieczeństwa ZBP

FinCERT.pl - Bankowe Centrum Cyberbezpieczeństwa ZBP funkcjonuje w ramach Zespołu Bezpieczeństwa Banków Związku Banków Polskich i gromadzi, analizuje oraz przekazuje w ramach sektora bankowego i we współpracy z organami ścigania oraz innymi instytucjami informacje dotyczące możliwych zagrożeń o charakterze przestępczym, godzącym w bezpieczeństwo banków oraz ich klientów.