

OSTRZEŻENIE PRZED ZAGROŻENIAMI **- oszustwo metodą na „wnuczka”/ „policjanta”/ „CBŚ”**

W związku z nasilającymi się zagrożeniami ze strony oszustów stosujących metody socjotechniczne po raz kolejny ostrzegamy przed próbami wyłudzeń metodą na „wnuczka”/ „Policjanta”/ „CBŚ”.

Standard tego typu procederu zawsze jest ten sam i polega na nakłonieniu ofiary do wykonania określonych czynności skutkujących najczęściej przekazaniem środków finansowych przestępcom.

Każdorazowo w tego typu przestępstwach **stosowane są metody polegające na przedstawieniu ofierze "wiarygodnej" informacji skłaniającej ją do wykonania określonych czynności**. Za pomocą różnych technik manipulacyjnych przestępcy próbują pozyskać od upatrzonych wcześniej ofiar dane, dzięki którym możliwe jest podjęcie pieniędzy z ich rachunków bankowych.

Najczęstsze scenariusze:

1. **metoda "na wnuczka"** - często motywem przewodnim jest próba wykorzystania nieprawdziwej informacji o osobie bliskiej np. o chorobie, wypadku, problemach z prawem, pobycie w szpitalu, konieczności zapłaty odszkodowania, itp. – w tego typu przypadkach celem działania przestępców jest najczęściej pozyskanie środków finansowych (najczęściej w formie gotówki), które zgodnie z przygotowanym wcześniej scenariuszem ataku mają zniwelować skutki jednego z w/w fikcyjnych zdarzeń;
2. **metoda "na Policjanta/ CBA/ CBŚ/ prokuratora"** - często motywem przewodnim jest próba wykorzystania nieprawdziwej informacji o zagrożeniu środków na rachunku bankowym (np. informacja o włamaniu do konta, ataku hakerskim na bank, kradzieży środków z rachunku, itp.) - najczęściej celem tych działań jest nakłonienie ofiary do nawiązania "współpracy" z oficerem w/w służb w prowadzonej akcji mającej na celu zatrzymanie oszustów.

Elementem tej "współpracy" jest najczęściej wskazanie na konieczność:

- 1) przekazania środków:
 - w formie gotówkowej oficerowi, który ma się skontaktować osobiście;
 - w formie gotówkowej we wskazanym miejscu i czasie (np. pozostawienie pieniędzy w paczce);
 - w formie bezgotówkowej na wskazanym (telefonicznie lub mailowo) rachunek bankowy.
- 2) przekazania loginów, haseł, środków uwierzytelniających umożliwiających przestępcy dokonanie przelewu pieniędzy. Gdy ofiara nie posiada elektronicznego dostępu do rachunków bankowych, przestępcy często nakłaniają ją do wystąpienia do swojego banku z wnioskiem o kanały elektroniczne. Otrzymane z banku loginy i hasła przekazywane są przestępcom. Czasem dochodzi do takiej sytuacji, że ofiara podaje dodatkowo numer telefonu wskazany uprzednio przez przestępcę, by umożliwić autoryzację przelewów.

W tego typu próbach sprawcy często przedstawiają historię o rzekomym rozpracowywaniu grup hakerskich, często fałszywie wskazując na zaangażowanie w proceder pracowników banków, uwiarygadniają swoją historię prosząc ofiarę o potwierdzenie danych rzekomego policjanta dzwoniąc

na nr alarmowy 997, tymczasem rozmowa jest przekierowywana do przestępcy, który potwierdza nazwisko, nr legitymacji osoby podszywającej się pod policjanta.

Często wykorzystywanym elementem dodatkowym przy tego typu atakach jest:

- zastraszenie ofiary koniecznością poniesienia odpowiedzialności (karnej, finansowej, itp.) za niepowodzenie akcji policyjnej spowodowane brakiem współpracy z jej strony;
- "przetrzymywanie" ofiary na połączeniu telefonicznym co ma dodatkowo potęgować stres i uniemożliwić jakikolwiek próby weryfikacji otrzymanych informacji.

Przypominamy:

- bądź ostrożny w kontakcie z nieznanym – nigdy nie podawaj podczas rozmowy swoich danych osobowych, loginów i haseł do bankowości internetowej oraz danych kartowych;
- nigdy nie przekazuj pieniędzy osobom, których nie znasz. Nie ufaj osobom, które telefonicznie podają się za krewnych lub ich przyjaciół. Jeśli dzwoni do Ciebie osoba podająca się za kogoś bliskiego i prosi o przekazanie Twoich oszczędności, najlepiej rozłącz się i zgłoś tę sytuację osobiście w najbliższej jednostce policji;
- jeśli masz wątpliwości czy rozmawiasz z wnuczką lub inną bliską osobą, rozłącz się i zadzwoń do nich samodzielnie. Nigdy nie oddzwaniaj na numer podany podczas rozmowy telefonicznej.
- Policja nigdy nie prosi telefonicznie o udział w działaniach operacyjnych;
- Policja nigdy nie prosi o przekazywanie pieniędzy ani kosztowności nieznanym osobom;
- Jeśli ktoś telefonicznie prosi nas o pieniądze, udział w akcji policyjnej bądź mamy jakiegokolwiek wątpliwości, z kim rozmawiamy, należy skontaktować się z najbliższymi. Jeżeli nie ma takiej możliwości, a podejrzewamy, że ktoś próbuje nas oszukać, natychmiast trzeba się skontaktować z policją, dzwoniąc na 997 lub 112 – najlepiej z telefonu komórkowego, ewentualnie stacjonarnego po uprzednim upewnieniu się, że ostatnia rozmowa została rozłączona. To bardzo ważne!