KPP W SOKOŁOWIE PODLASKIM

https://mazowiecka.policja.gov.pl/wsk/aktualnosci/58692,Oszustwa-finansowe-uwazaj.html
2021-12-09, 01:37

OSZUSTWA FINANSOWE – UWAŻAJ!

Data publikacji 10.09.2021

Wciąż nie maleje liczba dokonywanych oszustw w celu przejęcia środków finansowych czy kosztowności. Apelujemy, by nie odbierać niechcianych połączeń telefonicznych ani nie aktywować nieznanych linków otrzymywanych w wiadomości e-mail, sms czy innych komunikatorach.

Uważaj:

zadzwonił ktoś z rodziny z prośbą o pieniądze, które pilnie potrzebuje – tak działają oszuści!

zadzwonił ktoś, kto podał się za funkcjonariusza CBŚP i twierdzi, że Twoje oszczędności są zagrożone... - rozłącz się i poinformuj Policję - to oszustwo!

przyszedł mężczyzna, który przedstawił się jako funkcjonariusz, by odebrać pieniądze – to na pewno oszustwo!

Uwaga!

Wysoką aktywność wykazują oszuści podający się za pracowników banku czy policjanta. W przykładowej rozmowie telefonicznej:

oszust mówi, że pieniądze na koncie bankowym są zagrożone i trzeba potwierdzić swoje dane do logowania. Rozmowa jest prowadzona, aby ostatecznie podać obcej osobie dane wrażliwe. Wtedy przestępcy mają możliwość dokonania przelewu za pomocą wygenerowanego kodu, albo dysponowania środkami finansowymi po zalogowaniu się na to konto bankowe.

w przypadku oszustw typu „na wnuczka” rozmowa prowadzona jest w taki sposób, aby oszukiwana osoba uwierzyła, że rozmawia z kimś ze swojej rodziny i sama wymieniła jego imię oraz inne dane, pozwalające przestępcom wiarygodnie pokierować dalszą rozmowę. Sprawcom zależy, aby skłonić ofiarę do przekazania pieniędzy nieznajomemu, mimo że będzie widziała go po raz pierwszy w życiu.

Nigdy nie należy wierzyć w takie historie! To oszustwa!

„Na blika”:

oszustwo z wykorzystaniem systemu płatności mobilnych (BLIK), które polega na wyłudzeniu kodu do autoryzacji przez telefon przed podszywanie się pod znajomych w mediach społecznościowych. Oszuści zdobywają najpierw hasła do profilu kont naszych znajomych. Logują się w serwisie, a potem nawiązują z nami kontakt. Proszą o podanie kodu "blik", umożliwiającego dokonanie płatności elektronicznej wyjaśniając, że właśnie stoją przy kasie i chcą zapłacić za zakupy, ale ich karta akurat w tym dniu straciła ważność itp.

„Na kryptowaluty”:

oszuści wykorzystując fałszywe serwisy internetowe, podszywają się pod pośredników i oferują ułatwienia w inwestowaniu. Przestępcy nakłaniają potencjalnych pokrzywdzonych do przekazania pieniędzy, obiecując wysokie i szybkie zyski bez ryzyka. Proponują pomoc przy inwestowaniu. Dla uwiarygodnienia informacji w banerze reklamowym m.in. były wykorzystywane wizerunki znanych osób, które miały się na nich wzbogacić. Po wypełnieniu formularza kontaktowego, z osobami zainteresowanymi inwestowaniem kontaktował się wtedy fałszywy konsultant, który - najczęściej posługując się obcym akcentem - wyjaśniał, jak działa strona i jak w szybki sposób można zarobić.

„Na zdalny pulpit”:

za pomocą właśnie takiego oprogramowania można zostać bez oszczędności! Cyberoszuści pod pretekstem łatwego zysku, inwestycji w kryptowaluty lub w ramach „konsultacji bankowych” polecają instalację takiego programu, przejmując przy jego użyciu kontrolę nad naszymi urządzeniami, na których logujemy się do swoich banków. Wówczas wystarczy tylko chwila, aby nasze konto bankowe zostało „wyczyszczone”. Osoby, które się na to zdecydowały, były namawiane do instalowania na swoim komputerze ogólnodostępnego oprogramowania, a tym samym udostępniali zawartość pamięci swojego dysku oraz umożliwiali dostęp do bankowości internetowej. Ostatecznie zamiast zysków, z ich kont znikały wszystkie zgromadzone tam środki.

Uwaga!

Oszuści wyłudzający pieniądze dbają o każdy szczegół podczas rozmowy i stosują coraz bardziej wyszukane socjotechniki np.: na telefonie klienta wyświetlają numer infolinii banku oraz używają nazwisk rzeczywistych pracowników banków.

Oszuści podszywają się pod osoby zainteresowane kupnem towarów wystawianych na portalach sprzedażowych. Udając potencjalnego klienta oferują zapłatę wysyłając specjalny link – gdzie należy podać login i hasło do własnego konta bankowego. W ten sposób skradzione dane poufne służą do przechwytywania oszczędności.

Oszuści przysyłają sms-y z linkiem do odsłuchania nowej poczty głosowej, które są przekierowaniem na fałszywe strony internetowe.

Apelujemy, aby korzystając z obecnych technologii stale dbać o znajomość zasad bezpieczeństwa w sieci i zapewniać ochronę swoich danych oraz za każdym razem weryfikować tożsamość osób, które kontaktują z prośbą o pieniądze czy inne dane.

Każde zdarzenie lub próbę wyłudzenia zgłoś w najbliższej jednostce Policji lub zadzwoń na 112.

Dodatkowo każdy może zgłosić stronę, co do jakiej ma podejrzenie, że może wyłudzać dane osobowe, dane uwierzytelniające do kont bankowych lub serwisów społecznościowych do Zespołu CERT Polska. W przypadku, gdy źródłem podejrzanej strony jest wiadomość SMS zawierający link, można go przesłać na numer 799-448-084 wykorzystując funkcję „przekaż” albo „udostępnij” w swoim telefonie. Do zgłaszania incydentów służy także formularz dostępny na https://incydent.cert.pl/phishing.

Wydział Prewencji KWP /SSz/MG/