Oszustwa nowych technologii to plaga obecnych czasów. Przestępcy internetowi korzystając z własnej wiedzy oraz niewiedzy i naiwności swoich ofiar wykorzystują okazje do kradzieży w sposób całkowicie bezlitosny. Szczególnie niebezpieczne i bardzo podstępne jest oszustwo na AnyDesk.

Program komputerowy AnyDesk stosowany jest w świecie cyfrowym od wielu lat. Jego główną funkcją jest zdalny podgląd pulpitu na innym komputerze i możliwość jego przejmowania w celu wykonywania czynności. Program jest bardzo przydatny w pracy. Gdy jest wykorzystywany w dobrych celach ułatwia i przyspiesza wykonywanie wspólnej pracy. Ale niestety jest on również wykorzystywany przez oszustów.

Musimy pamiętać, że oszustwo na AnyDesk nigdy nie występuje samodzielnie, a jedynie jest elementem innego oszustwa internetowego. Występuje wspólnie z takim przestępstwem, jak oszustwo na Bitcoiny. Procedura zazwyczaj wygląda następująco: Z ofiarą kontaktuje się oszust (telefonicznie, czy też za pomocą komunikatorów społecznych). Podaje się za „eksperta" w dziedzinie inwestowania cudzych pieniędzy i obiecuje ofierze ponadprzeciętne zyski z inwestycji, głównie w kryptowaluty. Gdy oszust namówił ofiarę do zainwestowania pieniędzy, żąda od niej podania danych osobowych i namawia ją do zainstalowania na swoim urządzeniu programu AnyDesk, by mogła widzieć, jak „broker" inwestuje i pomnaża włożone przez nią pieniądze. Niestety ofiara nawet nie orientuje się, że instalując program AnyDesk spowodowała, iż oszust internetowy korzysta z jej pulpitu i uzyskuje wgląd w jej loginy i hasła. Zazwyczaj oszust następnie prosi swoją ofiarę, aby weszła na swoje konto internetowe i przelała jakieś środki na „rachunek inwestycyjny". W tym momencie oszust dokonuje operacji.

Jak uniknąć oszustwa na AnyDesk? Najważniejsze to nie instalować żadnego oprogramowania na swoich urządzeniach, gdy żąda tego dzwoniąca lub pisząca do nas obca osoba, która podaje się za „eksperta" czy „brokera". Instytucje takie, jak banki, firmy telekomunikacyjne czy urzędy nie wymagają od swoich klientów/petentów instalowania dodatkowego oprogramowania. Tym bardziej, jeśli skutkiem instalacji będzie możliwość podglądu pulpitu i możliwości zdalnego wykonywania operacji na naszym urządzeniu.

Apelujemy o ostrożność i rozsądek. Zarówno w świecie realnym, jak i wirtualnym, stosujemy zasadę ograniczonego zaufania i nikomu nie udostępniamy danych logowania do naszych rachunków bankowych. Oszuści cały czas wykorzystują metodę „na zdalny pulpit". Kradzież pieniędzy odbywa się na oczach pokrzywdzonych. Internetowi przestępcy najpierw skłaniają ofiarę do zainstalowania programu zdalnej obsługi komputera, a potem polecają, by zalogowała się do swojego konta w banku.