**AnyDesk és egyéb távoli asztal elérést biztosító programok által végrehajtott csalás módszer:**

A csalás azzal kezdődik, hogy a bank nevében telefonáló „gyanús pénzügyi mozgásra” hivatkozik számlaszámunkon és ennek további megakadályozására vírusirtót vagy új számlanyitást javasol. Valójában a távoli hozzáférést biztosító AnyDesk programot telepíttet a hívott fél mobiljára vagy számítógépére azért, hogy aztán annak segítségével megszerezzék az illető pénzét.

 A sértett ebben az esetben nem ad meg semmilyen banki azonosítót, ezért nem is érti, hogyan veszíti el a pénzét. Egy „banki app” telepítésének tudatában van.

Részletesen: Először a csalók arra kérnek, hogy a Google Play vagy App Store telefonos alkalmazásokban keressük meg az AnyDesk applikációt. A legjobb, ha már ennél a pontnál nemet mondunk, és bontjuk a vonalat. Ha azonban ezt nem tesszük meg, és az alkalmazást mégis megkeressük, akkor a következő képernyőkép látszik:

Ezután a csaló arra kér, hogy telepítsük a programot és indítsuk el. 

**Mondjunk nemet!**

Ha nem mondunk nemet, akkor a telepítéshez először elfogadtatják velünk az adatvédelmi nyilatkozatot, majd a következő ablakban végig vezetnek az alkalmazás 4-5 oldalas „bemutatóján”, és az alábbi, kikerülhetetlen információkon:





AnyDesk felülete:

Ezután kéri, hogy adjuk meg a távoli hozzáféréshez szükséges egyedi „Az Ön címe” kódot.

Ne adjuk meg az egyedi kódot! A csaló a kód ismeretében távolról csatlakozni tud a telefonunkhoz vagy számítógépünkhöz, vagyis mindent lát, ami a készüléken beírunk. Ez alapján szerzi meg jelszavunkat az internetes bankunkhoz! Csatlakozás előtt a telefonunkon, megjelenik egy figyelmeztető ablak a kötelező 5 másodperces késleltetéssel (a kulcsátadást is megjelenítve). Ha ezt meglátjuk, szakítsuk meg a folyamatot! A csaló ezután azt kéri, hogy az „Ismerem a kockázatokat” jelölőnégyzetet válasszuk ki. Semmiképpen ne jelöljük be a négyzetet, mert az elkövetők csak ezzel a hozzájárulással tudnak hozzáférni a telefonunkhoz.

Ha figyelmesen elolvassuk a képernyőképen található a magyarázatot, láthatjuk, hogy itt is jelzik, egy idegen személynek adunk hozzáférést készülékünkhöz:

A következő ablakban pedig arra kérnek, állítsuk be, hogy a csaló milyen jogosultsággal férhessen hozzá a telefonunkhoz.

Itt lehet kiválasztani az opciókat. Ha a fentieket mégis elfogadjuk, és tovább megyünk, akkor lesz még egy komoly figyelmeztető üzenet.

Ne nyomjunk rá, hogy „Indítás most”, mert kattintás után létrejön a kapcsolat és a csaló mindent lát, sőt akár az irányítást is átveheti a telefonunk vagy ha arra telepítettük, az asztali gépünk felett.

Ezt követően az internetes banki belépő oldalra terelnek minket. Kérik, hogy telefonban ne mondjuk be az adatokat csak gépeljük be a felületre. Az belépő oldalon beírt számlaszámot, jelszavakat és kódokat a csaló is látja és az képen rögzíti. Ezután a csaló is képes belépni az internetes bankfiókunka és egyéb, minden információ megszerzésére is képes lesz amit a telefonunkon tárolunk.