KRIMI

Vigyázat! Csalók élnek vissza a Gyermekklinika nevével

Megjelent: 2020.04.02. 11:27
Szerző: **Nikolényi Gábor Viktor**

A szegedi Gyermekklinika a közösségi oldalán adta hírül, hogy többen is adománygyűjtésbe kezdtek a klinika nevében, holott az intézmény semmilyen gyűjtést nem kezdeményezett.

„Tudomásunkra jutott, hogy a Gyermekklinika nevével visszaélve többen pénzadomány gyűjtésbe kezdtek. A Gyermekklinika semmilyen gyűjtést nem kezdeményezett, nem folytat! Egyik módszerük, hogy futárt küldenek a készpénzért a Gyermekklinikára hivatkozva. Kérem, amennyiben ilyet tapasztalnak, jelentsék a Rendőrségnek” – olvasható a bejegyzésben, amelyet Dr. Bereczki Csaba írt a Gyermekklinika Facebook-oldalán.

Szeged Gyermekklinika
csütörtökön

Tisztelt Szülők!

Tudomásunkra jutott, hogy a Gyermekklinika nevével visszaélve, többen pénz adomány gyűjtésbe kezdtek. A Gyermekklinika semmilyen gyűjtést nem kezdeményezett, nem folytat! Egyik módszerük, hogy futárt küldenek a készpénzért, a Gyermekklinikára hivatkozva. Kérem, amennyiben ilyet tapasztalnak, jelentsék a Rendőrségnek. (A megosztásokat köszönjük.)

Köszönettel:... Továbbiak

64 Hozzászólok 3,2 E

Úgy tűnik, hogy a szélhámosok a koronavírus-járvány miatti félelmet kihasználva egyre gátlástalanabb módon próbálnak pénzhez jutni. Szerdán a Nemzeti Kibervédelmi Intézet honlapján megjelent egy cikk arról, hogy a csalók hamis e-mailekkel próbálkoznak és ez akár a bejelentkezési adatokat is veszélybe sodorhatja.

Írásuk szerint a támadók helyi kórházak nevében küldenek e-maileket, amelyekben azt állítják, hogy a címzett érintkezett egy olyan kollégával, baráttal vagy családtaggal, akinél kimutatták a koronavírus-fertőzést. Ezért arra kérik a felhasználót, hogy a mellékelt űrlap kitöltése és kinyomtatása után fáradjon be a legközelebbi kórházba a tesztek elvégzéséhez.

Kiemelték: ha valaki megnyitja a mellékletként küldött “EmergencyContact.xlsm” táblázatot, és rákattint a “Tartalom engedélyezése” gombra, káros szoftvert letöltő és lefuttató makrók indulnak el az áldozat gépén. A rosszindulatú program egyrészt felderíti a megtámadott rendszert (könyvtármegosztások, telepített programok), másrészt kriptopénztárcákat (kriptopénzek tárolására szolgáló program) és a böngészők által elmentett sütiket (cookie) próbál megszerezni: így a bejelentkezési adatok is veszélybe kerülhetnek – hangsúlyozták.

FRISS