SZEMÉLYESADAT-LOPÁS A KÖZÖSSÉGI MÉDIÁBAN

A csalók különböző módszerek alkalmazásával megpróbálják elérni, hogy Ön megadja személyes adatait (név, e-mail cím, jelszó, hitelkártyaszám stb.). Ezt annak ellenére is megtehetik, hogy Ön megfelelő védelmet alkalmaz, közösségimédia-fiókjainak tartalmát nem láthatja mindenki, vagy ha óvatosságból nem oszt meg túl sok információt a profiljában (olyanokat, amelyekkel ellophatják a személyazonosságát). Az adatok birtokában aztán jóvá nem hagyott vásárlásokat hajthatnak végre az Ön hitelkártyájával, bankszámlát nyithatnak; telefon-előfizetést vásárolhatnak; hitelt vehetnek fel; illegális üzleti tranzakciókat hajthatnak végre; eladhatják adatait más csalóknak.

Mit tegyen személyes adatai védelme érdekében?

- Rendszeresen tekintse át közösségimédia-fiókjai adatvédelmi és biztonsági beállításait! Áldozzon némi időt annak a megismerésére, hogy mit mutat a profilja Önről a külvilág számára!
- Gondolja át alaposan, hogy mennyi információt és fényképet oszt meg a közösségimédia-oldalakon! Felhasználásukkal a csalók hamis személyazonosságot hozhatnak létre, vagy megpróbálhatják átverni.
- Végezzen online kutatást! Keressen rá az adott termék nevére vagy a munkaajánlatra, és nézze meg, mit mondanak a többiek! Használjon olyan szavakat a keresőkifejezésben, mint „felülvizsgálat”, „panasz” és „csalás”!
- Jelentse a közösségimédia-platform üzemeltetőinek azokat a profilokat, amelyekről azt gyanítja, hogy csaláshoz hozták létre őket! Tiltsa le őket, ha az ismerősei vagy a követői, és szakítson meg velük minden kapcsolatot!
- Ha valódi ismerőseitől kap szokatlan vagy gyanús üzenetet, illetve lát általuk közzétéve furcsa posztot, gyanakodjon és jelentse a közösségimédia-platform üzemeltetőjének!
- Ellenőrizze rendszeresen a hitelkártyája és a betéti kártyája kivonatait! Ha olyan dologért terhelték meg a számláját, amelyet nem Ön rendelt meg, vegye fel a kapcsolatot a bankkal és a kártyatársasággal!

Egyéb, a fentiekben nem részletezett csalási formák:

- **Pharming**: a támadás során az áldozat eszközére rosszindulatú kódot telepítenek, ami figyeli és gyűjti a bejelentkezési adatokat (ilyennel lehet találkozni egy validnak tűnő alkalmazás (pl. játék) telepítése során is)
- **Evil twin phishing**: hamis Wi-Fi hálózat létrehozása, amely valódinak tűnik (ha valaki bejelentkezik, és bizalmas adatokat ad meg, a hacker rögzíti az adatait)
- **Angler phishing**: hamis közösségi média bejegyzések / hirdetések használata adatszerzésre (legtöbbször ráveszik az áldozatot arra, hogy töltsön le valamit, vagy kattintson egy linkre)
- **Social engineering**: ez a klasszikus átverős, megtévesztős, manipulálós dolgok gyűjtőneve (sok a fentiek közül ide is tartozik)

forrás: https://kiberpajzs.hu/ kép internet