# Nógrád Vármegyei Rendőr-főkapitányság

## Óvja meg értékeit a netes csalóktól!

**Tisztelt Internetfelhasználó!**

Manapság az internetes technológiákat körülbelül négymilliárdnyian használják személyes, illetve üzleti célokra, például információkeresésre, szolgáltatások és áruk megrendelésére, kapcsolattartásra, szórakozásra. Azonban ne feledkezzünk meg arról, hogy ez a világ ugyanúgy rejtegethet veszélyeket, mint maga a való élet! Online csalók folyamatosan levelek, linkek, csábító ajánlatok megküldésével az óvatlan internethasználók pénzét próbálják megszerezni.

**Legyünk mindig óvatosak!!!**

### A legelterjedtebb csalási formák:

**Telefonos:** olyan telefonos csalás, amelynél a támadó megpróbálja személyes, pénzügyi vagy biztonsági információi megosztására vagy pénz átutalására rávenni az áldozatokat, akik általában banki ügyfelek. A vishing tipikus formája, amikor a csaló az adathalász hívás során megpróbálja elhitetni a felhasználóval, hogy ténylegesen egy banki alkalmazottal beszél, és egy pénzügyi tranzakció során fellépett hiba vagy csalásgyanú miatt telefonál.

**Számítógépes:** a fogyasztók és a vállalkozások egyre többet vásárolnak és adnak el az interneten. Nézzen utána a dolgoknak: vásárlás előtt keressen rá a hirdetőre, olvasson értékeléseket, ismertetőket az adott termékről!
Kizárólag biztonságos fizetési szolgáltatásokkal fizessen! Gyanakodjon, ha pénzküldési szolgáltatás használatát kérik!

**SMS:** A smishing (az angol „SMS” és „phishing”, vagyis SMS és adathalászat szavak kombinációja) olyan csalás, amelynél a támadók SMS segítségével próbálnak megszerezni személyes, pénzügyi vagy biztonsági adatokat, információkat. Megbízható forrásnak álcázzák magukat, úgy tesznek, mintha egy bank, kártyakibocsátó, futárszolgálat, közműszolgáltató vagy valamilyen egyéb szolgáltató képviseletében jelentkeznének. Az üzenet arra kéri a címzettet – általában sürgető módon –, hogy nyisson meg egy weboldalra vezető hivatkozást, telepítsen egy alkalmazást, vagy hívjon fel egy telefonszámot például a fiókja ellenőrzése, frissítése vagy újraaktiválása érdekében. A hivatkozás hamis weboldalra mutat, a telefonszámon pedig egy csaló jelentkezik, aki az adott cég munkatársának adja ki magát.

**Email:** ez az adathalász csalási forma olyan, banki ügyfeleket célzó, csaló szándékú e-mail, amely személyes, pénzügyi vagy biztonsági információi megosztására próbálja rávenni a címzettet. Ezek a levelek azonosnak tűnhetnek azokkal az üzenetekkel, amelyeket a létező bankok küldenek: a csalók lemásolják a valódi e-mailek logóit, kinézetét és stílusát, esetenként korábbi (hamis vagy valós) levélváltások részleteit is tartalmazzák.

Bővebb információk: www.kiberpajzs.hu

**Előzze meg, hogy pénzét, adatait az elkövetők megszerezzék!**
**A bankok telefonon soha nem kérnek teljes bankkártya adatokat, cvc kódot, jelszót.**

Kérjük, fogadja meg tanácsainkat! Különösen banki adatait, azonosítóit ne adja meg idegeneknek! Banki internetes oldal helyett használja a pénzintézet mobil applikációját, mert a csalók által készített banki oldalak megtévesztésig hasonlítanak az eredetiekhez. Ha azt tapasztalja, hogy a jó azonosító adatok megadása után értesítést kap, hogy nem megfelelő a bejelentkezés, akkor valószínűleg egy áloldalt hívott le és a csalók így akarják megszerezni adatait.

**Ha úgy érzi adatait megszerezték, azonnal keresse meg bankját!**

**Biztonságos böngészést kívánunk!**

Hasznos tanácsokért kövesse a Nógrád Vármegyei Rendőr-főkapitányság Bűnmegelőzési Alosztály „Biztonság A Fő” facebook oldalát!!!

Bővebb információk: www.kiberpajzs.hu