

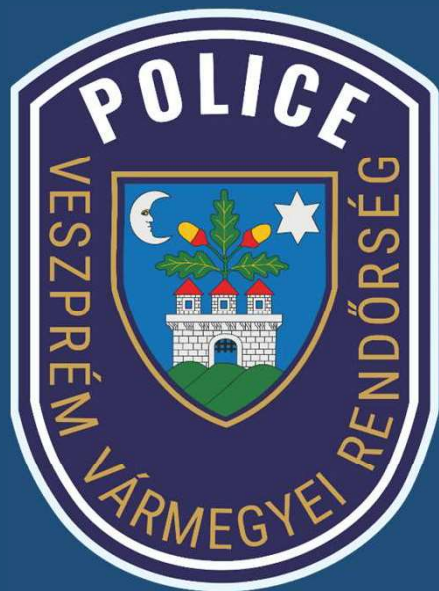


## BIZTONSÁGBAN A BALATONON

A sikeres térség egyik bástyája a biztonság!

Siófok 2024.03.07.

Az online térben elkövetett csalások típusai, jellemző módszerei,  
és a megelőzés lehetőségei

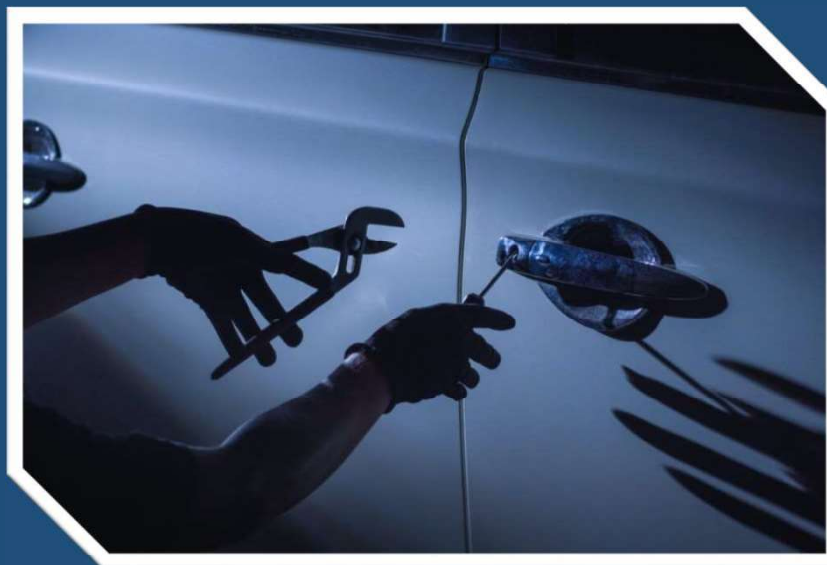


Suszter Tamás r.ezredes  
bűnügyi rendőrfőkapitány-helyettes



## Bevezető

Országosan és a térségben is egyértelmű tendencia, hogy a több éve csökkenő számú regisztrált bűncselekmények struktúrájában a közterületen elkövetett bűncselekmények, garázdaságok, testi sértések és az úgynevezett klasszikus vagyon elleni bűncselekmények lopások, betöréses lopások, gépkocsi feltörések, rablások, kifosztások száma jelentős mértékben csökkent.





## Bevezető

Az elkövetett cselekmények jelentős része a valós térből az online térbe vándorolt. A bűnelkövetők naponta új és újabb módszerrel próbálkoznak, hogy a gyanútlan és felkészületlen áldozataikat behálózzák, személyes vagy digitális adataikat megszerezzék, annak érdekében, elsősorban azért, hogy vagyoni kárt okozzanak a sértettnek.





## Veszprém vármegyében regisztrált bűncselekmények szemléltetése



forrás: ENyÜBS  
elkövetés helye szerinti adatok



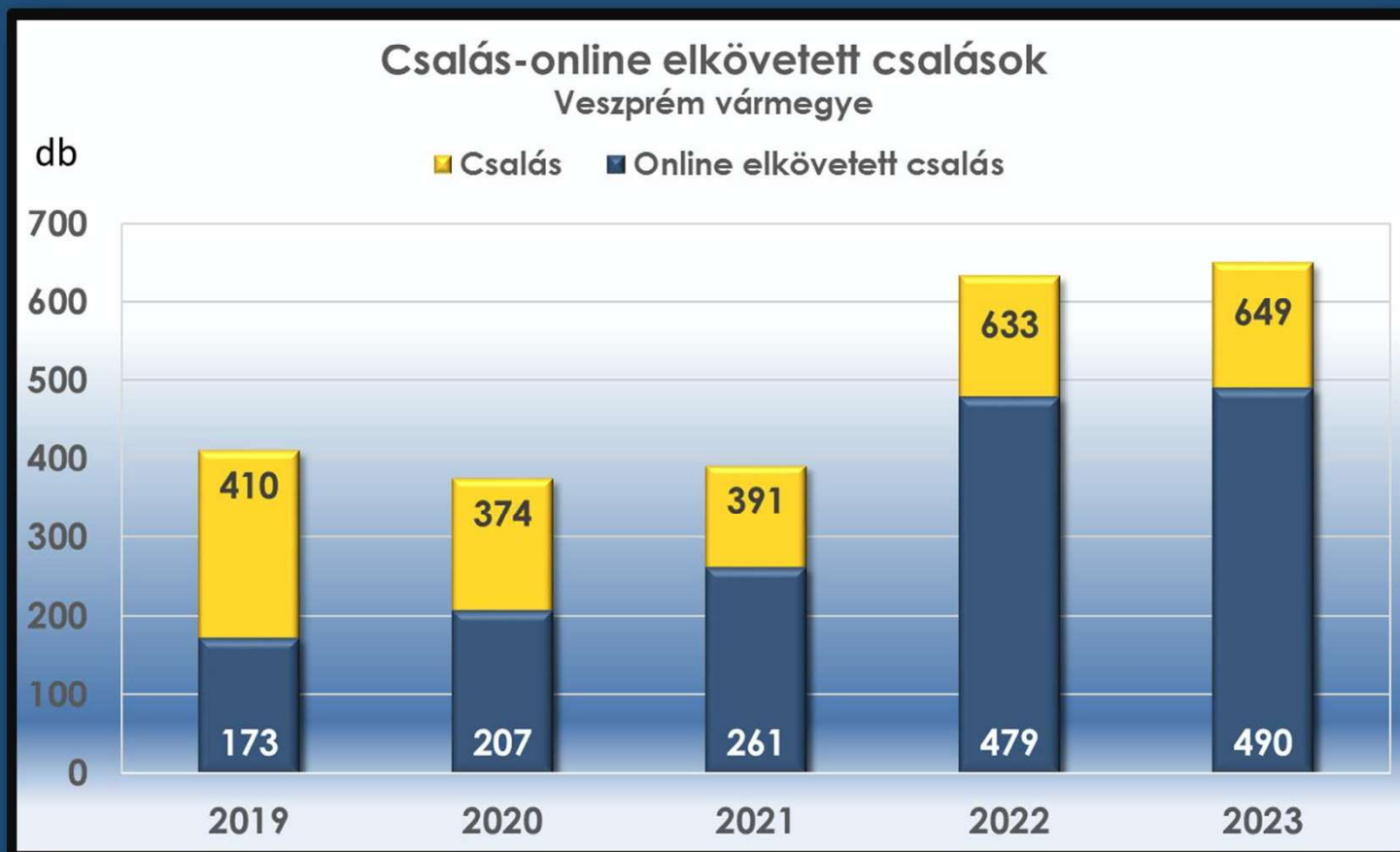
## lopás, rablás, kifosztás bűncselekmények szemléltetése



forrás: ENyÜBS  
elkövetés helye szerinti adatok



## Az online csalások szemléltetése



forrás: ENyÜBS  
elkövetés helye szerinti adatok



# Online térben elkövetett bűncselekmények

5 típusa különíthető el

Befektetési csalások

Pénzintézet nevében  
elkövetett csalások

Anydesk,  
Teamviewer

Online áruvásárlással,  
eladással kapcsolatos  
csalások

Marketplace,  
FoxPost, GLS, DPD,  
Posta

Szerelmi csalások

...egy Amerikában  
élő katona...

Számlaváltós csalások

Megváltozott  
számlaszámra  
hivatkozva...



## Befektetési csalás

Jellemzően hamis befektetési lehetőségeket kínálnak az elkövetők (főleg kriptovaluta)

Feljelentés érkezett ismeretlen tettes ellen: A feljelentő elmondta, hogy a facebook közösségi oldalon feltett jövedelmező, kriptovalutával összefüggő befektetési hirdetésre jelentkezett, felhívta a hirdetésben megadott telefonszámot, majd elutalta a befektetés összegét egy számára ismeretlen nevére szóló számlára. A feljelentőt százezer forint kár érte.





## A befektetési tárgyú csalások megelőzése

Széleskörű lakossági edukációs kampány folytatása a befektetési csalásokkal kapcsolatos veszélyek felhívása érdekében.

A pénzintézetek, befektetési alapokat kezelő szereplők célirányos, bűnmegelőzési, figyelemfelhívó kampányai, kiemelve, hogy rajtuk keresztül a befektetés minden esetben biztonságos.

Felhívás, hogy az interneten ismert vagy sikeres emberek nevével hirdetett befektetések nagy valószínűséggel csalások.

Az e-mail útján, szakmaiatlan és gyanút keltő stílusban érkezett befektetési javaslatokat, kapcsolatfelvételt minden esetben el kell utasítani.



## Pénzintézetek nevében elkövetett csalás

Képernyő megosztó (Anydesk, Rusk desk, Teamviewer) telepítésére és banki felületre belépésre rábírás.

Feljelentés érkezett ismeretlen tettes ellen: A feljelentő elmondta, hogy telefonon felhívta egy ismeretlen személy, aki magát banki alkalmazottnak kiadva tévedésbe ejtette azzal, hogy gyanús tranzakciókat észleltek a bankszámláján, illetve a folyamatban lévő tranzakciók megszakítása érdekében felajánlották a segítségüket. A feljelentő ijedt állapotában nem észlelte, hogy átverésről van szó, így rávették őt arra, hogy a mobiltelefonjára letöltse az Anydesk távoli elérést biztosító applikációt, majd az alkalmazásban látható kóddal létrehozták a távoli kapcsolatot. Az alkalmazás funkcióit kihasználva megszerezték a feljelentő számlaszámához tartozó internetbank fiók adatait, majd ezen internetes kapcsolat során pénzáttalást kezdeményeztek a sértett tudta és beleegyezése nélkül a netbankjából, mintegy 30 millió forint értékben.



## Pénzintézetek nevében elkövetett csalás





## A pénzintézet nevében elkövetett csalások megelőzése

Folyamatos oktatás és kommunikáció minden lehetséges csatornán

Ebbe be kell vonni minden lehetséges banki, közigazgatási szereplőt, lakossági és intézményi erőforrást

Gyanús elemek: a banki ügyintézők nem kapcsolják más pénzintézet munkatársát, nem ajánlanak nyereményjátékot és soha nem kérnek banki jelszavakat vagy teljes bankkártya adatokat.

Hiteles pénzintézeti kommunikációs csatornák alkalmazása

Legalapvetőbb tanácsok: ismeretlen programot ne telepítsünk, ne adjuk meg banki adatainkat senkinek és gyanú esetén azonnal szakítsuk meg a hívást.



## Az online áruvásárlással, eladással kapcsolatos csalások

Az elkövető felveszi a kapcsolatot a termék eladójával azon legendával, hogy megvásárolta a terméket és intézi a szállítást. Az elkövető email címet kér a sértettől, amelyre meghamisított-utánozott (fake) banki, szállítmányozó (Foxpost, GLS, DHL) vagy kereskedelmi oldalak (Vinted, Marketplace, Jófogás) cég nevében adathalász weboldalra vezető weblinket küld az elkövető, amelyet megnyitva a sértett megadja a banki adatait és engedélyező kódokat.



# Az online áruvásárlással, eladással kapcsolatos csalások

A link: <http://p-6-30-47-199.nyc.megapath.net/otp.hu/include.php>

Mozilla Firefox

Előzmények | Deletozás | Könyvtárak | Értékek | Súgó | Bejelentkezés

http://p-6-30-47-199.nyc.megapath.net/otp.hu/include.php

Rólunk | Kártya | OTP Csoport | Kapcsolat | Hírfelvi | English

otpbank

Keresés OK

Magánszemélyek | Kisvállalkozások | Vállalatok | Önkormányzatok | Befektetői kapcsolatok

Melyiket válassza?  
Mire is használhatja?

Botóli kártyák  
Hitelkártyák  
Tudja, mire használható egy bankkártya?

Akcióajánlatok  
Lekötések  
Értékpapírok  
Prémium vagyontervezés

Lakáscélú hitelek  
Szabad felhasználású hitelek

OTPdirekt telefonon  
OTPdirekt interneten  
OTPdirekt mobiltelefonon

Kártyaszámot:

ATM PIN kód:

Belépés

OTPdirekt

Egyenleglekérdezős

Számlakivonat lekérdezés

- Bankidőket és ATM-ek elérhetősége, szolgáltatásait
- Hirdetmény, Üzletszabályzat
- Kalkulátorok, keresők
- Online ügyintézés
- Befektetési jegy-árfolyamok
- Elérhetőségeink
- Aktuális és archiv befektetési közlemények
- OTP Hírfelvi, BANKÓ
- Próbálja ki mobilon is! mobil.otpbank.hu

OTP Junior  
A fiatalok bankja.

Private Banking  
A közvetlen kapcsolat.

Devizaárfolyamok



## Az online áruvásárlással, eladással kapcsolatos csalások megelőzése

A rendőrség, piaci szolgáltatók, webhelyek kezelőinek tájékoztatása a biztonságos online vásárlásról.

A tájékoztatás a konkrét veszélyekről: csomagküldő cégek nevével való visszaélés, ál web-oldalak létrehozása, vagy link küldése a bankkártya adatok megszerzése céljából.

Online vásárlás CSAK biztonságos webáruházból, lehetőleg előre utalás nélkül, ellenőrizhető módon történjen.

Vásárláskor SOHA sincs szükség : a megküldött linkre kattintásra, a bankkártya vagy banki adatok megadására a fizetés érdekében.

Az ún. „közösségi piactereken” kialakított profilok mögött bárki, akár fiktív személy is lehet.



## Nyomozócsoport megalakítása

2023. március 1-től nyomozó csoport alakult a Veszprém Vármegyei Rendőr-Főkapitányság Bűnügyi Igazgatóságán.

A nyomozócsoportba 2 fő került átrendelésre a városi rendőrkapitányságok állományából, továbbá az Elemző - Értékelő Osztály, Gazdaságvédelmi Osztály, Felderítő Osztály munkatársai is részt vesznek a működésben.



**A Bűnügyi Igazgatóság állománya  
jelenleg 45 online térben elkövetett  
csalással kapcsolatban folytat  
nyomozást**

**Fő ismérvek: gyorsaság, szakszerűség**





## Felderítési, nyomozási nehézségek

Kapcsolattartás a strómanokat irányító és a hívásokat koordináló személyek között üzenetküldő applikációkon (Telegram, Messenger) történik.

A pénzfelvétel rendkívül rövid idő alatt megtörténik, az elkövetők készülnek az átutalásra és azonnal intézkednek a felvételre (nagy összegnél előre jelzik a bankfiókban a pénzfelvételi szándékot).

A megtévesztő hívások és az informatikai műveletek a valódi IP címet elfedő VPN hálózatokon zajlik.

Banki biztonsági rendszerek gyors ügyintézése hivatali időn kívül, olykor hivatali időben is, személyes kapcsolatokon múlik.





## Központi támogatás

Az Országos Rendőr-Főkapitányság augusztus 1-től a vármegyei rendőr-főkapitányságok állománytábláját módosította, így 3 fő hivatásos és 2 fő munkavállaló (informatikus) státusz betöltésére nyílt lehetőség.





# Bűnmegelőzés

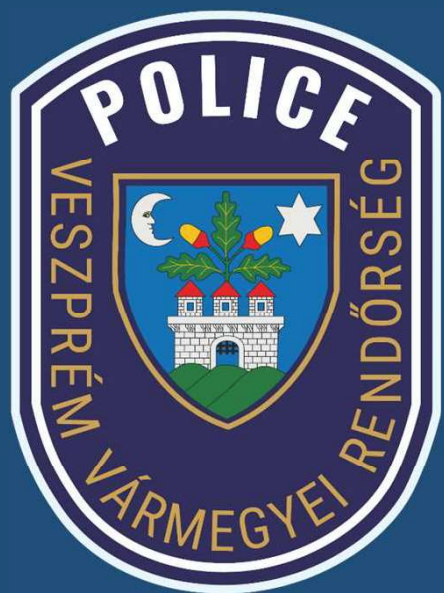
3 párhuzamosan működő bűnmegelőzési forma

Országos Rendőr-  
főkapitányság

Veszprém Vármegyei  
Rendőrfőkapitányság

„KiberPajzs”

- Edukáció (lakosság, üzleti szereplők, jogi személyek, stb.)
- Minden társadalmi szereplőhöz eljuttatni a preventív információt
- Kommunikáció minden lehetséges csatornán és módon
- Változatos formában történő folyamatos ismeretátadás
- Aktualitásokon alapuló naprakész bűnmegelőzési munka



**Köszönöm a figyelmet!**