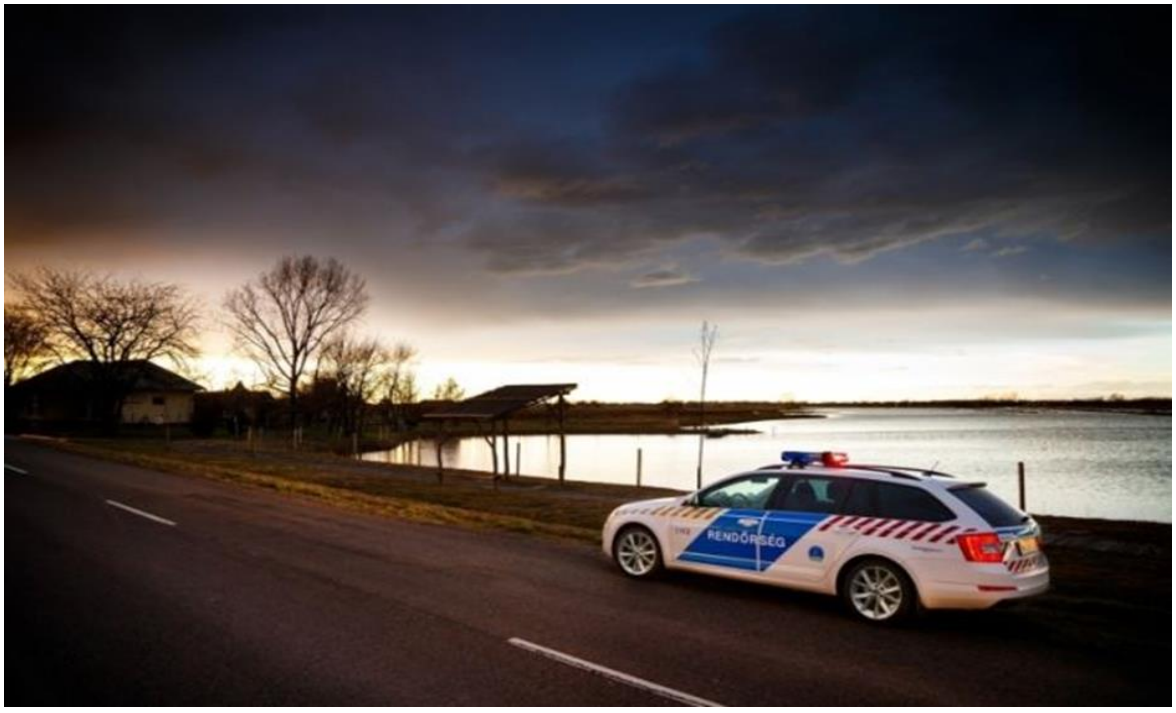
GYŐR-MOSON-SOPRON MEGYEI RENDŐR-FŐKAPITÁNYSÁG
BŰNMEGELŐZÉSI OSZTÁLY

ELBÍR HÍRLEVÉL



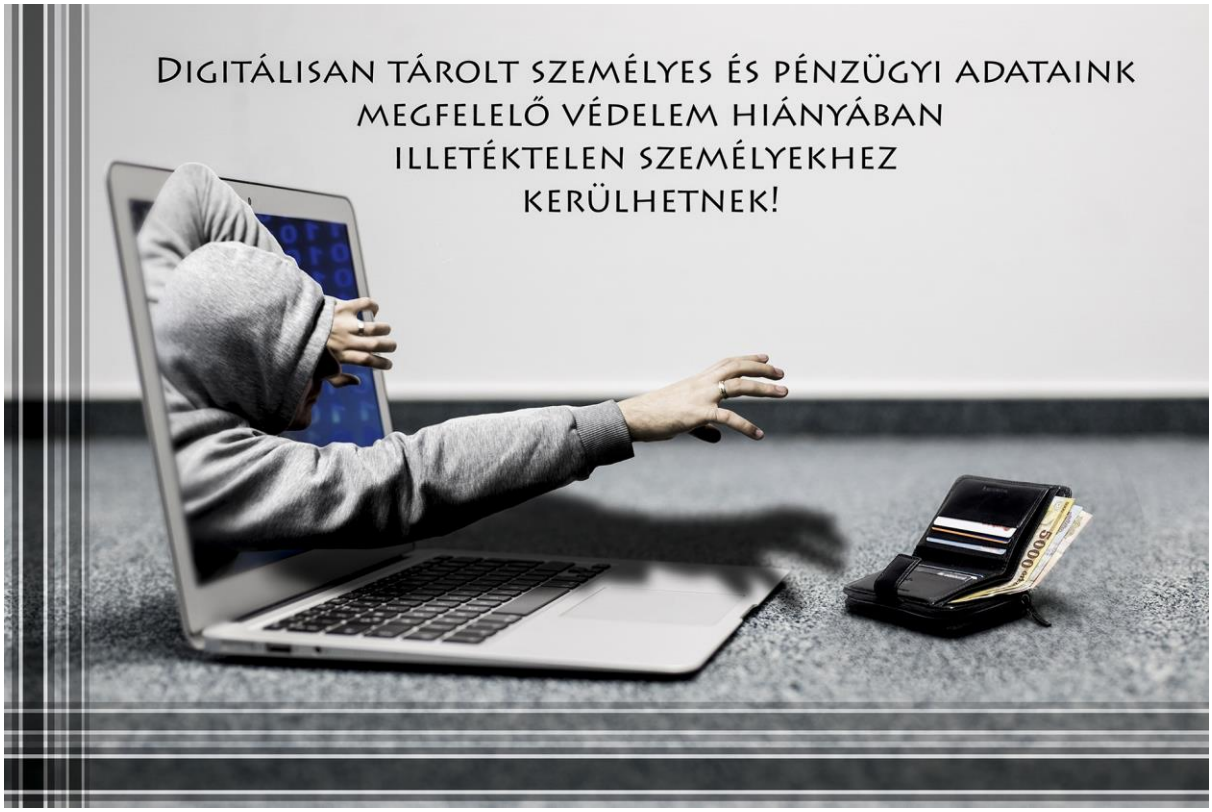
Tisztelt Olvasó!

A Győr-Moson-Sopron Megyei Rendőr-főkapitányság **2019. februári** havi bűnmegelőzési hírlevelét olvassa. A hírlevelet az Országos Rendőr-főkapitányságon a Rend és Biztonság Közbiztonsági Program rendőrségi feladatainak végrehajtására kiadott feladatterv szerint készítjük el Önöknek minden hónapban. Ha úgy gondolja, hogy nem szeretne a későbbiekben a hírlevelünkből kapni, kérem, elektronikus formában jelezze részünkre és a címlistából törölni fogjuk. A hírlevelet a megyénkben dolgozó bűnmegelőzési munkatársaink által megküldött az adott hónapra vonatkozó tipikus bűncselekményekről szóló – tájékoztatók alapján készítjük el. A leírt bűncselekmények egy bizonyos megyei településen történtek, de gyakorlatilag bárhol megtörténhettek volna.

Amennyiben a hírlevél tartalmát hasznosnak ítéli – a forrás megjelölésével! –, bátran felhasználhatja a lakosság tájékoztatására (pl. képújság a helyi TV-ben, önkormányzati intézmények faliújságai, stb.). Reméljük ezzel is hozzájárulhatunk ahhoz, hogy az Ön településének lakói minél kevesebb számban váljanak bűncselekmények áldozatává. Hírleveleinkben, a hétköznapi életben gyakran előforduló, illetve aktuálisan megtörtént bűncselekményekre, illetve azok megelőzési lehetőségeire hívjuk fel a figyelmet.
tagállamában –, minden év februárjának második keddjén, ugyanazon a napon rendezik meg. E-havi hírlevelünket ennek szellemében készítettük el Önöknek.

Cím: 9024 Győr, Szent Imre u. 2-4. Pf.: 302 9002
Telefon: (96) 520-020, BM: 21/14-76, Telefax: (96) 520-000/15-69, BM: 21/15-69
E-mail: bunmeg.gyormrfk@gyor.police.hu

BIZTONSÁGOS INTERNETHASZNÁLAT



A technikai fejlődés következtében az internet a mindennapok része lett. Használatával könnyebbé, egyszerűbbé tehetjük életünket. A virtuális tér azonban valós veszélyeket is jelent. Digitálisan tárolt személyes és pénzügyi adataink megfelelő védelem hiányában illetéktelen személyekhez kerülhetnek. Az elkövetők módszerei időről-időre változnak, de az ajánlott biztonsági intézkedések és magatartási szabályok tudatos betartásával jelentősen csökkenthetőek a felmerülő kockázatok.

BIZTONSÁGOS KÖRNYEZET

A technikai megoldások, akár csak az otthonunk védelmében, jelentik az első lépcsőt. Gondoskodjunk arról, hogy a számítógépünk és az otthoni hálózatunk is biztonságos legyen. Ennek érdekében:

·Rendszeresen telepítse számítógépén az operációs rendszer és a felhasználói programok frissítéseit. Mobileszközein is frissítse az alkalmazásokat!

·A vírusok (és egyéb kártékony programok) elleni védekezés céljából feltétlenül javasolt vírusirtó program telepítése és frissítése!

·Számítógépén a felhasználói fiókok felügyeletén állítsa be, hogy a kritikus műveletekhez (pl. program telepítése) a felhasználó engedélyére legyen szükség!

·Ne állítsa a böngésző biztonsági beállításait az „ajánlott” szint alá!

·Ismeretlen eredetű szoftvereket ne telepítsen!

TUDATOS INTERNETHASZNÁLAT

A legjobb zár és riasztó sem ér semmit, ha tulajdonos átadja a kulcsot és a kódot, vagy nyitva hagyja az ajtót és nem kapcsolja be a riasztót. Az interneten keresztül érkező veszélyek néhány egyszerű szabály betartásával elkerülhetőek:

·Csak ismerős feladó által küldött e-mail mellékletét nyissa meg!
·Soha ne adjon meg jelszót, PIN kódot e-mailben küldött kérésre!
·Belépéskor mindig gépelje be az URL címet, ne a kapott linkre kattintva lépjen be az oldalra!
·Online történő bankkártyás fizetésnél mindig győződjön meg arról, hogy valódi bank oldalon adja meg az adatokat, más oldalon (pl. kereskedő oldalán) ne adja meg azokat!
·Felhasználói nevet és jelszót csak tanúsítvánnyal rendelkező (https előtag) oldalon adjon meg!

ADATAINK FOKOZOTT VÉDELME

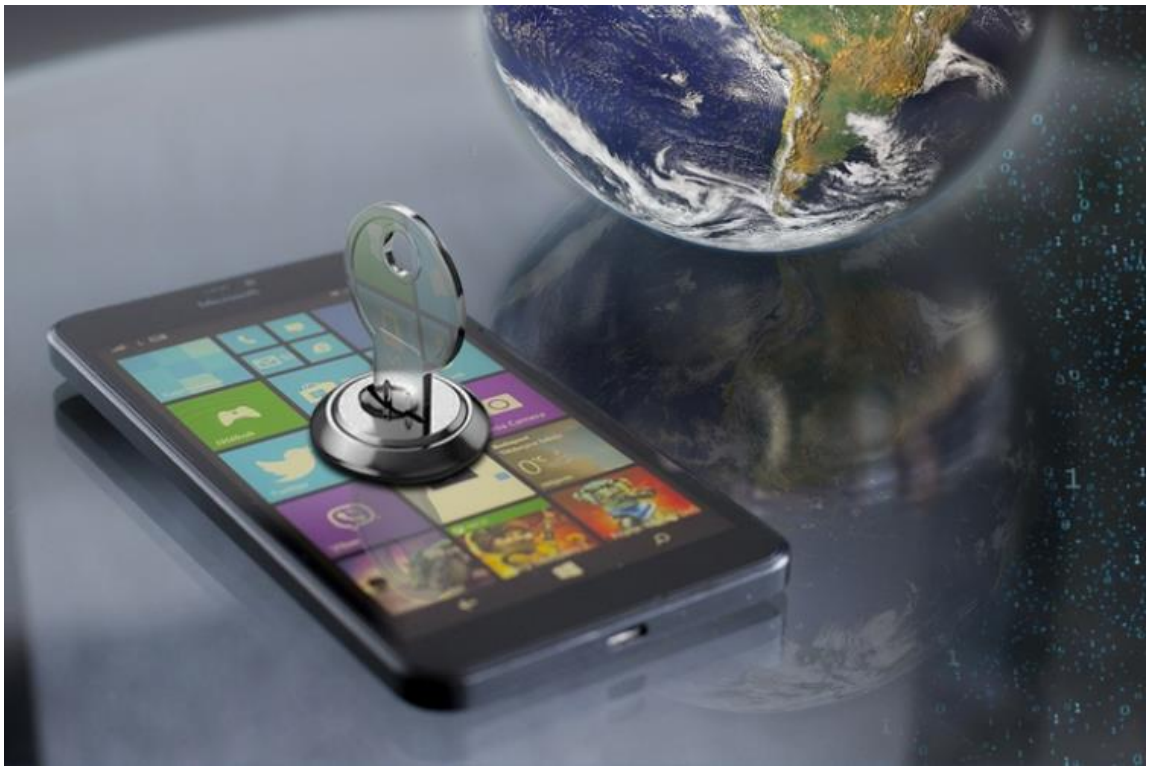
Otthon az értékeink (készpénz, ékszer) védelmére további megoldásokat (értéktároló, széf) használunk. A digitálisan tárolt adatainkat védelme érdekében is fokozott körültekintéssel járjunk el: egyrészt, hogy illetéktelen személyek ne férjenek hozzá, másrészt elvesztésük (pl. technikai probléma, szándékos károkozás) esetén is vissza tudjuk állítani őket:

·Ne adja meg senkinek felhasználói nevét és jelszavát!
·Közösségi oldalon ne legyen nyilvános a profilja, a személyes adatait, a megosztott tartalmakat csak az ismerősei láthassák!
·Csoportosítsa ismerőseit és ezáltal korlátozhatja, hogy ki mit láthat!
·Egyéb oldalra vagy alkalmazásba közösségi profiljával történő bejelentkezés során ellenőrizze, hogy az oldal vagy alkalmazás milyen személyes adatához fér hozzá. (születésnap, e-mail cím, ismerőseinek köre stb.)! Szükség esetén módosíthatja az elérhető információk körét.
·Más által is használt számítógépen - ha befejezte az internet használatát - minden esetben jelentkezzen ki a közösségi oldalról, levelezéséből! A böngésző bezárása nem elegendő.
·Rendszeresen készítsen biztonsági másolatot fontos adataikról. Erre alkalmas lehet egy külső merevlemez, amit csak a biztonsági mentés idejére csatlakoztatunk a számítógéphez vagy olyan online tárhely, amely tárolja a fájlok korábbi verzióját is.

100%-os biztonság nincs!
DE!
A biztonságos környezet megteremtésével, tudatos internethasználattal és adatainak fokozott védelmével biztonságosabbá tehetjük az internethasználatot.

Biztonságos internethasználatért: mobileszközök biztonsága

A mobileszközök (okostelefonok, táblagépek) jelentősen megkönnyítik mindennapjainkat. Mivel azonban nem csak otthon vagy munkahelyünkön használjuk, nagyobb a kockázata, hogy illetéktelen kezekbe kerülnek.



Bizalmas és személyes adatokat tárolunk rajtuk, ezért elvesztésük vagy ellopásuk esetén az illetéktelen személyek hozzáférhetnek az eszközön tárolt üzenetekhez, fényképekhez, videókhoz, személyes és bankkártya adatokhoz, valamint a banki és közösségi oldalak bejelentkezési adataihoz. Az illetéktelen hozzáférésből adódó kockázatok elkerülése érdekében gondoskodjunk mobileszközeink megfelelő védelméről.

KÉPERNYŐZÁR

Ha az eszközünk illetéktelen személy kezébe kerül, megfelelő védelem hiányában bárki könnyen hozzáférhet adatainkhoz. Ennek megelőzésére a legegyszerűbb, ha alkalmazza az automatikus képernyőzárat, így ha nem használja az eszközt, az előre beállított idő után a képernyőzár automatikusan bekapcsol. A telefon feloldásához használja készüléke lehetőségei közül az Ön számára legmegfelelőbb megoldást: kódszám, jelszó, ujjlenyomat stb. Ajánlott bekapcsolni a PIN-kód kérését is.

TÁVOLI FELÜGYELET BEÁLLÍTÁSA

A távoli felügyelet használata esetén – amennyiben az eszköz be van kapcsolva és csatlakozik az internethez – lehetőség van az eszköz helyének térképen történő megjelenítésére, illetve szükség esetén, az eszközön tárolt felhasználói adatok és beállítások törlésére.

Az ehhez szükséges applikáció az ismert alkalmazásboltokból letölthető.

FRISSÍTÉSEK ÉS BIZTONSÁGI BEÁLLÍTÁSOK

Frissítse mobileszközei operációs rendszerét minél előbb az erre vonatkozó figyelmeztetést követően. Az alkalmazások esetében engedélyezze, hogy automatikusan frissítsék magukat.

Ezek ugyanis olyan kritikus biztonsági réseket javíthatnak ki, amelyek hiányát a hackerek kihasználhatják rosszindulatú programok telepítésére, bizalmas adatok megszerzésére.

Amennyiben éppen nem használja a wifit vagy bluetooth-t, érdemes kikapcsolni, ezzel is korlátozhatja az eszköz illetéktelen elérését.

ADATOK BIZTONSÁGA

A mobileszközökön tárolt adatokhoz nemcsak az eszköz megszerzésén keresztül lehet hozzájutni. Sok alkalmazás menti és szinkronizálja az adatokat (fájlokat, beállításokat, jelszavakat) valamilyen online tárhelyre (más néven felhőbe).

Ez akár hasznos is lehet, hiszen az eszköz elvesztése vagy ellopása esetén az adatok nem vesznek el. Fontos azonban, hogy a szinkronizáció csak a tudtával és belegyezésével történjen. Ha nem tartja szükségesnek az adott alkalmazásban az adatok szinkronizálását, akkor azt tiltsa le.

BIZTONSÁGOS ALKALMAZÁSOK

A mobileszközökön futó alkalmazások – a részükre biztosított engedélyektől függően – hozzáférhetnek a személyes adatokhoz, fájlokhoz, fényképeket, videókat, hangfelvételt készíthetnek, ezeket továbbíthatják az alkalmazás készítőinek.

- A mobilalkalmazásokat mindig hivatalos alkalmazás-áruházból töltse le! Ellenőrizze, hogy az eredeti alkalmazásról van-e szó! A bűnözők ugyanis hasonló neveket használnak, hogy megtévesszék a felhasználókat.
- Üzenetben kapott linkről ne töltsön le alkalmazásokat!
- Letöltés előtt ellenőrizze az alkalmazás és a gyártó értékelését is. Szánjon rá időt és olvassa el a felhasználók véleményét. Válasszon olyan alkalmazást, amit többen töltöttek le és pozitív értékeléssel bír.
- Ellenőrizze, hogy milyen engedélyeket kér az alkalmazás. Ha nem tartjuk szükségesnek, akkor ne töltse le.

(Például: navigációs programoknak szükségük lehet hozzáférni a telefon helyzetéhez, de egy zenelejátszónak már nem).

BIZTONSÁGOS HASZNÁLAT

- A böngészőbe soha ne mentse el a felhasználói nevét, jelszavát. Használjon jelszókezelő alkalmazást!
- A böngészőben megjelenő figyelemfelhívások (például: az eszköz fertőzött, töltsön le vírusirtót, az eszköz elavult, frissítse) célja, hogy valamilyen kártékony programot telepítsen az eszközre. Ilyen esetben ne töltsön le semmit, és zárja be a böngészőt!

Tanulságos esetek

1. eset

Kisebb kárt okozó csalás vétség gyanúja miatt, a sértett feljelentése alapján eljárás indult ismeretlen tettes ellen, aki a sértett által interneten megrendelt bútor vásárlási vételi árából 80.000 Ft-ot előleg gyanánt elutaltatott a feljelentővel, ám a bútort nem szállította ki, azóta elérhetetlenné vált.
A bűncselekménnyel okozott kár: 80.000 Ft

Legyenek gyanakvóak az internetes hirdetési oldalakon tömegével található, **"hihetetlen ajánlatoknak"**, akár valamilyen termékről, műszaki cikkről, akár csábító munkalehetőségről van szó, mert ezek között rengeteg a csalók által létrehozott valótlan tartalmú hirdetés, amelyekkel a csalók ilyen módon akarnak pénzt szerezni áldozatuktól.

Soha, semmilyen internetes ajánlat, vásárlás során **ne fizessenek előre, ne küldjenek pénzt**, csak miután megkapták a terméket, és ellenőrizték, hogy tényleg azt kapták-e, amit rendeltek. Ha csak egy kicsit is gyanúsnak tűnik az üzlet, inkább mondjanak le róla!

Még a **postai utánvét sem elég biztonságos**, mert mielőtt a címzett kinyitná a csomagot, fizetni kell a postásnak, és csak ez után tudhatja meg, hogy tényleg az van-e a csomagban, amit rendelt.

A tapasztalatok alapján az egyetlen biztonságos vásárlási mód, ha miután az interneten megegyeztek az eladóval, egy megbeszélt helyen személyesen találkoznak, és miután személyesen meggyőződtek a termék, ajánlat létezéséről, valódiságáról, működőképességéről, csak azután fizessenek érte.

Ha az eladó nem akar személyesen találkozni, attól elzárkózik, halogatja a találkozót, váratlanul lemondja a megbeszélt találkozót, vagy nem jön el, gyanakodjon, mert nagy a valószínűsége, hogy csalóval van dolga!

Árubemutatók a gyakorlatban

1. Potenciális érdeklődők megkeresése

- A szórólapos invitálás eltűnőben van, helyette telefonon hívják a potenciális vásárlókat. Az árubemutatók fő célcsoportját az időskorú nyugdíjas, betegségekkel küzdő lehetséges vásárlók jelentik.

2. Bemutatók helyszínei

-2016-tól az árubemutatókról szóló szigorú szabályokat a cégek úgy kívánják elkerülni, hogy ezeket a rendezvényeket bejelentett, **orvosi rendelőnek kinéző üzletben** tartják meg, így megfosztják a fogyasztót az elállási jogtól. Ezen túl bemutatókat tartanak még **üzlethelyiségen kívül** például: étterem, kultúrház, szálloda. Új jelenségként **magánlakásokon** is tartanak, amely az idősek sérelmére elkövetett bűncselekmények miatt komoly veszélyt jelent. Ez utóbbi két típusú helyen szervezett bemutató esetén a fogyasztót megilleti a 14 napos elállási jog.

3. Az érdeklődők „szűrővizsgálata”

- A fogyasztóvédelmi hatóság által lefolytatott ellenőrzések tapasztalatai alapján elmondható, hogy jelenleg az árubemutatóval egybekötött termékértékesítést végző vállalkozások körében a legelterjedtebb gyakorlat, hogy a bemutatókat úgynevezett „ingyenes állapotfelmérésként”, „egészségügyi szűrővizsgálatként”, „egészségnapként” stb. hirdetik meg, az említett időskorú célcsoportra tekintettel. A „szűrővizsgálatokat” általában olyan személyek végzik, akik orvosnak adják ki magukat, ilyen végzettség nélkül.

4. A kapott eredmények „kiértékelése”

- Az ingyenes egészségügyi szűrést követően, **a mérési adatok kiértékelése után** – a rendkívül rossz értékekre, a fogyasztók rossz egészségi állapotára hivatkozva – a „probléma megoldását jelentő” **terméket kínálnak** a jellemzően idősebb korosztályhoz tartozó fogyasztók részére.

5. A termék bemutatása

- A következő lépés a termékek bemutatása, a termék „jó” tulajdonságainak részletezése, nem egy esetben beépített vagy magát orvosnak kiadó személy bevonásával, aki saját magán kívánja bemutatni a termék „csodás” gyógyhatását, állapotjavító hatását, ezzel is vásárlásra buzdítva a résztvevőket.

6. A termék árának a kifizetése

-2016 előtt a szervezők a helyszínen – hitelközvetítőkként – nyomban fogyasztási hitelszerződéseket kötöttek.
- Ma már a készpénzes fizetés jellemző, illetve a vállalkozás felajánlja, hogy **saját gépkocsiján bankba, bankautomatához kíséri vagy hazaszállítja a vásárlót**, aki a lakásán fizetheti ki a terméket.

7. A vásárlás után

- Az ellenőrzési tapasztalatok alapján egyértelműen megállapítható, hogy a cégek csak az értékesítésről szóló szerződés megkötéséig, illetve a termék átadásáig készségesek. Később, amikor érkeznek a jelentős összegű törlesztési csekkek és a vásárló szeretne a terméktől és a hiteltől megszabadulni, akkor a cég már elérhetetlenné válik.

8. Mit tud tenni a fogyasztó?

- Javasoljuk, hogy a fogyasztó üzleten kívüli értékesítés esetén a vételtől számított 14 napon belül éljen az az elállási jogával. Ha ez nem vezet eredményre, akkor forduljon a fogyasztóvédelmi hatósághoz, hatósági eljárás indítása céljából, ahol segítséget kaphat az egyedi igénye érvényesítéshez szükséges békéltető testületi eljárás megindításához is. Javasoljuk továbbá a rendőrség felkeresését is, ahol fogyasztók megtévesztése, vagy kuruzslás miatt tehetnek feljelentést.

9. A fogyasztóvédelmi ellenőrzések tapasztalatai

- A fogyasztóvédelmi hatóság által 2017-ben végzett ellenőrzés első időszakában összesen **19 esetben** végeztek helyszíni hatósági ellenőrzést. *A szabályozás megelőzően az árubemutatókkal kapcsolatban a fogyasztóvédelmi hatóság munkatársai 2015-ben éves szinten 180 hatósági ellenőrzést végeztek.* Ezek az eredmények is mutatják ezen jelenség visszaszorulását, egyre csökken ugyanis a fogyasztóvédelmi hatóság által ellenőrzés alá vonható bemutatók száma.
- Az eredményes fellépés következménye, hogy míg 2015-ben az árubemutatós cégekkel szemben átlagosan havi 43 panasz érkezett, 2016-ban 26 panasz, addig 2017-ben ez a szám átlagosan havi 13-ra csökkent.

10. Együttműködéssel az árubemutatókkal szemben

- Az árubemutatókkal szembeni eredményes fellépés érdekében az NFM Fogyasztóvédelemért Felelős Helyettes Államtitkársága által kidolgozott **árubemutató akcióterv** kerül megvalósításra.
- A fogyasztóvédelmi hatóság, a békéltető testületek, illetve a rendőrség együttműködésével eredményesen fel lehet lépni az árubemutatós cégek tevékenységével szemben.
- Az akcióterv alapján, tehát más tárcák és hatóságok is bevonásra kerülnek ezen témakör kezelése érdekében. Az árubemutatók ellenőrzését a fogyasztóvédelmi hatóság a társszervekkel együtt (népegészségügy, munkavédelem, munkaügy, NAV) folytatja le.

Nemzeti Fejlesztési Minisztérium

Nemzeti Adó- és Vámhivatal

RENDŐRSÉG POLICE

Fogadják meg tanácsainkat!
Előzzük meg együtt a bűncselekményeket!

Győr, 2019. február 08.

Tisztelettel:

Kovács Sándor r. alezredes
osztályvezető

Lelki Elsősegély Telefonszolgálat

„A szolgáltatásnak köszönhetően a hívó fél egy embertársával oszthatja meg problémáit, elfogadó, nem ítélkező légkörben. A szolgáltatás lelki támaszt nyújt magányos, lelki traumát átélő vagy az öngyilkosságot fontolgató hívók számára.”

A lelki elsősegély telefonszolgálat elérhető bárhonnan, vezetékes és mobiltelefonról európai rövidített hívószámon – **116-123** – díjmentesen és névtelenül éjjel-nappal Magyarország területéről.

HÉKI VONAL
GYERMEKKRÍZIS ALAPÍTVÁNY

116-112