Elektronikus Lakossági Bűnmegelőzési Információs Rendszer
ELBIR
LAKOSSÁGI HÍRLEVÉL

2020. július
BUDAPEST

Tisztelt ELBIR Olvasóink!

Júliusi számunkban folytatjuk az Országos Rendőr-főkapitányság Bűnmegelőzési Osztálya által összeállított, havonta jelentkező, többrészes, internetbiztonsággal foglalkozó sorozatunkat.

Az előző havi, a biztonságos internethasználatról szóló számunk után ezúttal egy, a számítógépünk védelmét célzó tájékoztatót juttatunk el Önökhöz.

Kérjük, ha tehetik, osszák meg hírlevelünket rokonaikkal, ismerőseikkel és szomszédjaikkal!

Hírlevelünkhöz kellemes olvasást és hasznos időtöltést kívánunk Önöknek!

A Budapesti Rendőr-főkapitányság Bűnmegelőzési Osztálya

H-1139 Budapest, Teve utca 4-6. Telefon: (+36-1) 443-5000,
BM telefon: 32-778, BM fax: 32-782, E-mail: elbir@budapest.police.hu, bunmeg.brfk@budapest.police.hu

Elektronikus Lakossági Bűnmegelőzési Információs Rendszer
ELBIR
LAKOSSÁGI HÍRLEVÉL

2020. július
BUDAPEST

Ön a Budapesti Rendőr-főkapitányság havonta jelentkező ELBIR (Elektronikus Lakossági Információs Rendszer) hírlevelét olvassa, melynek virtuális hasábjain minden hónapban egy adott téma köré csoportosuló bűnmegelőzési tanácsainkat osszuk meg Önökkel. Kövesse minden hónapban hírleveleinket! Amennyiben a Magyar Rendőrség hivatalos álláspontját, valamint közleményeit tartalmazó hivatalos forrásra van szüksége, kérjük, látogasson el a www.police.hu weboldalra. Ha Önnek a Rendőrség segítségére van szüksége, kérjük, tárcsázza a 112-es segélyhívót.

A Rendőrségi Adatvédelmi Nyilvántartás alapján az Elektronikus Lakossági Bűnmegelőzési Információs Rendszer (ELBIR hírlevél, a www.police.hu-n jelenleg Bűnügyi Hírlevélként nyilvántartott) kiküldése során, a hírlevélhez csatolni kell az „Érintetti tájékoztatót", amely az alábbi linken érhető el: http://www.police.hu/adatvedelmi-tajekoztatok/hu!a-rendorsegrol!adatvedelem!bunugy!korozes!bunugyi-hirlevel

Amennyiben a jövőben nem kívánja igénybe venni a BRFK ELBIR szolgáltatását, nem tart igényt hírlevelünkre, abban az esetben felénk, küldőkhöz (elbir@budapest.police.hu) intézett elektronikus levélben bármikor kérheti e-mail címe törlését.

H-1139 Budapest, Teve utca 4-6. Telefon: (+36-1) 443-5000,
BM telefon: 32-778, BM fax: 32-782, E-mail: elbir@budapest.police.hu, bunmeg.brfk@budapest.police.hu

Elektronikus Lakossági Bűnmegelőzési Információs Rendszer
ELBIR
LAKOSSÁGI HÍRLEVÉL

2020. július
BUDAPEST

A Budapesti Rendőr-főkapitányság telefonszámai:

A BRFK Központi száma: 06 (1) 443-5000
Központi segélyhívó: 112

BRFK BŰNMEGELŐZÉSI OSZTÁLY elérhetőségei:
Telefon: 06 (1) 443-5000/ 32-778 **Központi e-mail cím:** bunmeg.brfk@budapest.police.hu
BRFK drog-prevenciós összekötő tisztek elektronikus levélcíme: infodrog@budapest.police.hu
BRFK SMS-vonal hallássérülteknek: 06 (20) 9000-107
Telefontanú (anonim módon, 24 órában hívható, ingyenes zöld szám): 06 (80) 555-111

Kerületi kapitányságok, rendőrőrsök:

I.	kerületi Rendőrkapitányság	Tel.: 061-457-5600
II.	kerületi Rendőrkapitányság	Tel.: 061-346-1800
III.	kerületi Rendőrkapitányság	Tel.: 061-430-4700
	Rendőrőrs Békásmegyer	Tel.: 061-243-2511
IV.	kerületi Rendőrkapitányság	Tel.: 061-231-3410
	Rendőrőrs Káposztásmegyer	Tel.: 061-231-3446
V.	kerületi Rendőrkapitányság	Tel.: 061-373-1000
VI.	kerületi Rendőrkapitányság	Tel.: 061-461-8141
VII.	kerületi Rendőrkapitányság	Tel.: 061-461-8100
VIII.	kerületi Rendőrkapitányság	Tel.: 061-477-3700
	Rendőrőrs Keleti pályaudvar	Tel.: 061-477-3726
IX.	kerületi Rendőrkapitányság	Tel.: 061-455-4800
X.	kerületi Rendőrkapitányság	Tel.: 061-263-7200
XI.	kerületi Rendőrkapitányság	Tel.: 061-381-4300
	Rendőrőrs Őrmező	Tel.: 061-381-4331
XII.	kerületi Rendőrkapitányság	Tel.: 061-457-5650
XIII.	kerületi Rendőrkapitányság	Tel.: 061-236-2800
	Rendőrőrs Újlipótváros	Tel.: 061-236-2824
XIV.	kerületi Rendőrkapitányság	Tel.: 061-461-8150
	Rendőrőrs Alsórákos	Tel.: 061-461-8186
XV.	kerületi Rendőrkapitányság	Tel.: 061-231-3450
XVI.	kerületi Rendőrkapitányság	Tel.: 061-407-8455
XVII.	kerületi Rendőrkapitányság	Tel.: 061-253-2300
XVIII.	kerületi Rendőrkapitányság	Tel.: 061-292-9200
XIX.	kerületi Rendőrkapitányság	Tel.: 061-292-9250
XX-XXIII.	kerületi Rendőrkapitányság	Tel.: 061-421-1800
	Rendőrőrs Soroksár	Tel.: 061-421-1842
XXI.	kerületi Rendőrkapitányság	Tel.: 061-427-4600
XXII.	kerületi Rendőrkapitányság	Tel.: 061-229-2652
	Dunai Vízirendészeti Rendőrkapitányság	Tel.: 061-203-9132

SZÁMÍTÓGÉPÜNK VÉDELME

Az internet használata során számos veszély fenyegeti a felhasználókat és számítógépeiket. Ezekkel szemben a megfelelő biztonsági intézkedésekkel és magatartási szabályok tudatos betartásával lehet védekezni. Az aktuális kiadványunkban ezeket a veszélyeket és az ellenük való védekezés módjait mutatjuk be.

#AutomatikusFrissítés #RosszindulatúSzoftverek #Vírusirtó #Tűzfal #BiztonságiMentés

A SZÁMÍTÓGÉP MEGFELELŐ BEÁLLÍTÁSA

A **rosszindulatú szoftverek és hackerek** a számítógépen futó szoftverek (operációs rendszer és egyéb programok) biztonsági hibáit használják ki. A szoftverek gyártói az ismertté vált hibákat rendszeresen javítják, és a javításokat **frissítések kiadásával** juttatják el a felhasználókhoz. A frissítések kiadásával az addig esetleg nem nyilvános hibákról is tudomást szerezhetnek a rosszindulatú szoftvereket készítők és a hackerek, így azok a rendszerek, amelyeken a hibákat javító frissítés nem történt meg fokozottan veszélyeztetettek lesznek.

Az operációs rendszer **automatikus frissítésének** bekapcsolásával biztosítható, hogy a számítógép a frissítés közzétételét követő legrövidebb időn belül megkapja a biztonsági frissítéseket. A felhasználói programok jelentős része szintén jelzi, hogy újabb verzió elérhető, ezek telepítése is ajánlott a fenti okok miatt.

BIZTONSÁGI TANÁCSOK

- Kapcsolja be az automatikus frissítéseket!
- Felhasználói fiókok felügyeletén állítsa be, hogy a kritikus műveletekhez (pl. program telepítése) a felhasználó engedélyére legyen szükség!
- Állítsa magasabb szintre a böngészők biztonsági beállításait!
- Ismeretlen eredetű szoftvereket ne telepítsen!
- Használjon vírusirtó programot!
- Kapcsolja be a tűzfalat a számítógépén vagy a routeren!
- Rendszeresen készítsen biztonsági mentést fontos adatairól!

VÍRUSIRTÓ PROGRAMOK

A vírusok (és egyéb kártékony programok) elleni védekezés céljából feltétlenül javasolt **vírusirtó program telepítése.**

A hagyományos vírusirtó programok adatbázisok alapján azonosítják a káros programokat. Az adatbázist a vírusirtó szoftver gyártója **rendszeresen frissíti**, a frissítéseket a legtöbb vírusirtó szoftver automatikusan letölti az interneten keresztül. Ez a reaktív védelem.

A modern vírusirtó programok beépített **elemző algoritmusok** segítségével – a programok kódjának elemzésével – azonosítják a vírusokat (heurisztikus védelem). Mivel egy új vírus megjelenése után több nap is eltelhet, amíg a vírusirtó program gyártója adatbázisát frissíti, addig a reaktív vírusirtó nem nyújt védelmet. A heurisztikus módszereket is alkalmazó modern vírusirtók viszont addig is védelmet nyújtanak a legtöbb kártevő ellen, amíg a frissítés megtörténik.

TŰZFAL

A tűzfal célja a privát (otthoni/vállalati) és a nyilvános (internet) **HÁLÓZAT ELKÜLÖNÍTÉSE**, továbbá annak biztosítása, hogy a hálózaton keresztül egy adott számítógépbe ne történhessen illetéktelen behatolás.

HARDVERES TŰZFAL: valamilyen fizikai eszköz, ami a privát és a nyilvános hálózat között monitorozza és szabályozza a bejövő és kimenő hálózati forgalmat a beállított tűzfal szabályoknak megfelelően. Korlátozott tűzfalként alkalmazható egy otthoni router is, megfelelően beállítva kellő védelmet nyújthat a külső támadások ellen.

SZOFTVERES TŰZFAL: a tűzfal szoftver a számítógépen fut. (pl. Windows beépített tűzfala), és a számítógép bejövő és kimenő hálózati forgalmát monitorozza és szabályozza. Alkalmazása akkor indokolt különösen, ha a számítógép közvetlenül - nem routeren keresztül - csatlakozik az internethez.

BIZTONSÁGI MENTÉS

RENDSZERESEN készítsünk biztonsági másolatot **FONTOS ADATAINKRÓL.** 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. Online tárhely esetében azért fontos a fájl verziók korábbi eltárolása, mert, ha zsarolóvírus támadás éri a gépet, akkor az automatikus szinkronizációnak köszönhetően a titkosított fájlok kerülnek az online tárhelyre is, de a vírus eltávolítását követően a legutolsó ép verziók visszaállíthatóak.