

## Az eltűnt gyermekek világnapja **Május 25.**

Az eltűnt gyermekek világnapján ma már számos országban emlékeznek az 1979. május 25-én New Yorkban eltűnt 6 éves kislányra, [Etan Patzra](#) és sorstársaira, hogy felhívják a figyelmet a gyermekek védelmének fontosságára.

Az elszökés, csellengés okai között számos olyan tényező szerepel, amivel a gyermek nehezen küzd meg. Ilyen a kortárs bántalmazás, iskolai eredmények miatti szorongás, családi konfliktusok, intézeti körülmények, szabályok elleni lázadás, életkori szorongások és félelmek, de az eltűnést kiválthatja a kalandvágy, a túlzott kontroll alóli menekülés, a tiltott dolgok kipróbálásának vágya, vagy éppen segélykiáltás a figyelemért, szeretetért.

Akármi is legyen a kiváltó tényező, az elszökő gyermekek fokozott veszélynek vannak kitéve, amit ők sokszor fel sem tudnak mérni. Kíváncsiságuk, vagy éppen érzékeny, instabil lelkiállapotuk olyan helyzetekbe sodorhatja őket, melyekben könnyen áldozattá válhatnak.

Míg a családból eltűnt gyermekkorúak 80 - 90 százaléka egy-két napon belül „hazatalál”, addig a gyermekvédelmi gondozási helyükről, intézetekből, családotthonokból, gyermekfaluból eltűnt gyermekek esetében már leginkább a rendszeresen ismétlődő szökés fordul elő. Főként ezekkel a sorozatos intézeti szökésekkel magyarázható, hogy a kiskorúakra kiadott eltűnés miatti körözések száma évente átlagosan 5-6-szorosa a felnőttkorúakénak.



### 116-000 Kék Vonal az eltűnt és bántalmazott gyermekekért

Ingyenesen hívható a nap 24 órájában, ha:

- azon gondolkozol, hogy elszöksz otthonról
- ha már „eltűntnek” számítasz, azt érzed, nem tudsz hazamenni, és nincs kivel beszélned
- Magyarországra jöttél és nem vagy a szüleiddel
- információd van egy eltűnt fiatalról
- eltűnt egy szeretted.

# Hírlevél

2021  
május



Szolgálunk és Védünk

A Csongrád-Csanád Megyei Rendőr-főkapitányság Bűnmegelőzési Osztályának tájékoztatója

## Figyeljünk gyermekünkre,

- hangolódjunk rá,
- adjunk neki időt a magunkéból, amikor igényli,
- hagyjuk, hogy a maga módján kibeszélje problémáit,
- tudjunk róla, mikor, hol tartózkodik, kikkel barátkozik, ismerjük baráti körének elérhetőségeit.

## Ha eltűnt,

- érdeklődjünk ismerőseinél, barátainál, járjuk be szokott helyeit, az eltűnést jelentsük be a rendőrségen, **kérjünk segítséget!**

## Központi segélyhívó szám rendőrségi bejelentéshez: 112

A rendőrség minden gyermek- és fiatalkorú eltűnését kiemelt fontosságú feladatként kezeli, azonban a jelenség kezeléséhez elengedhetetlen a problémakörben érintett gyermekvédelmi szervezetek, a civil kezdeményezések és családok együttműködése.

A gyermekeltűnések megelőzése közös társadalmi feladat. A felnövekvő generáció fokozott odafigyelést érdemel, különösen olyan időszakokban, amelyek az átlagosnál jelentősebb stresszterheléssel járhatnak, mint a bizonyítványosztás, a világjárvány miatti korlátozások és a digitális oktatás következtében átszerveződött kortárs kapcsolati rendszerek, napi rutinok, vagy a nyári iskolai szünet szabadsága, lazább kontrollja.

Ne feledjük, hogy a felnőttek adhatják a legnagyobb biztonságot a gyermekek számára!



Vigyázzunk egymásra, hogy ebben az évben is **együtt ünnepelhessük** május utolsó

vasárnapján a **gyermeknapot!**

**EGÉSZ ÉVBEN AZ ÖNÖK BIZTONSÁGA ÉRDEKÉBEN!**



Csongrád Megyei RFK - Bűnmegelőzési Osztály  
e-mail: [barka@csongrad.police.hu](mailto:barka@csongrad.police.hu)

112 – központi segélyhívó / rendőrségi segélyhívó - 107



## 2. 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.

### 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 készítő és a hackerek, így azok a rendszerek, amelyeken a hibákat javító frissítés nem történt meg, fokozottan veszélyeztetettek lehetnek.

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.

### 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 tevékenységének elemzésével – azonosítják a vírusokat. (heurisztikus védelem) Mivel egy új vírus megjelenése után több nap is eltelhet, amíg a vírusirtó program gyártója frissíti az adatbázist, 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 tűzfalszabályoknak 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.

## BIZTONSÁGI TANÁCSOK

- Kapcsolja be az operációs rendszer és a felhasználói programok **AUTOMAIKUS FRISSÍTÉSÉT**!
- A 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!

## TOVÁBBI INFORMÁCIÓK ÉRHETŐEK EL AZ ALÁBBI LINKEKEN



[www.police.hu/hu/hirek-es-informaciok/bunmegelozes/internet-biztonsag](http://www.police.hu/hu/hirek-es-informaciok/bunmegelozes/internet-biztonsag)



[www.facebook.com/internettudatosan](https://www.facebook.com/internettudatosan)