

SZÉCHENYI
2020



IT BIZTONSÁG

INFORMÁCIÓS FÜZET

SZÜLŐK
RÉSZÉRE

2021.

SZÉCHENYI 2020



MAGYARORSZÁG
KORMÁNYA

Európai Unió
Európai Szociális
Alap



BEFEKTETÉS A JÖVŐBE

Tartalom

Mi az az IT biztonság? Miért kell beszélni róla?	4
Gyermekünk és az internet	
Valódi kapcsolatok helyett virtuális kapcsolat	5
Mire használhatjuk az internetet?	6
1. Tanulás, ismeretszerzés	6
2. Kommunikáció, kapcsolattartás	6
3. Új lehetőségek, véleménynyilvánítás	6
4. Szórakozás	7
Beszélgünk őszintén az Internet veszélyeiről is!	8
1. Az ismerkedés veszélyei	9
2. Kamu oldalak, álhírek az interneten	10
3. Ami az internetre kikerült, annak örökre nyoma marad	11
4. Online zaklatás (cyberbullying), erőszak az interneten	12
5. Az internetes vásárlás veszélyei	14
6. Vírusok és kémprogramok	15
7. Életkornak nem megfelelő tartalmak	16
8. Felnőttek veszélyeztető magatartása	17
Programok, melyeket a gyerekeink használnak	18
I. Közösségimédia-oldalak	18
1. Facebook	18
2. Instagram	18
3. Snapchat	18
4. TikTok	19
5. Twitch	20
6. Discord	20
II. Azonnali üzenetküldő alkalmazások	21
1. WhatsApp	21
2. Viber	21
3. Messenger	22
III. Játékok	23

1.	Fortnite	23
2.	PUBG	24
3.	Roblox	25
4.	Brawl Stars	25
IV.	Gyermekek számára nem ajánlott anonim üzenetküldők	26
1.	Ask.fm	26
2.	Anotalk	26
3.	Tellonym	26
V.	Egyéb platformok, alkalmazások	28
1.	Reddit	28
2.	Tumblr	28
3.	Tinder	28
Ajánlott weboldalak:		31
Forrás:		31

Mi az az IT biztonság? Miért kell beszélni róla?

Mai felgyorsult világunkban rengeteg infokommunikációs eszközt használunk az otthonunkban, munkahelyünkön, ügyintézés közben. Netbankolunk, webáruházakban vásárlunk, szabadidőnkben közösségi oldalakat használunk, információkat osztunk meg másokkal.

A szolgáltatók törekszenek arra, hogy biztonságos környezetet teremtsenek számunkra, mégis egyre több veszélynek vagyunk kitéve, ha nem vagyunk kellőképpen körültekintőek. Nem csak mi, felnőttek használjuk az internetet és a különböző okoseszközöket, hanem gyermekeink is. Látszólag nagyon magabiztosan mozognak az online világban, de vajon ismerik-e annak veszélyeit? És mi szülők tudjuk-e, hogy milyen programokat használnak, milyen adatokat osztanak meg másokkal, kikkel barátkoznak, ismerkednek gyermekeink? Tudjuk-e hogyan védhetjük meg őket?

Gyermeink és az internet

Valódi kapcsolatok helyett virtuális kapcsolat

- Sok 3-4 éves gyerek kap ajándékba okoseszközt, amit hamarabb megtanul kezelni, mint a felnőttek. Ez elmagányosodáshoz vezethet, később is otthonosabban mozog a gyermek a virtuális világban, a valós kapcsolatokban nehezen ismeri ki magát.
- Fontos a személyes példa a családban - közös beszélgetések, játék, különböző vélemények megvitatása, társas viselkedés szabályainak megtanulása.
- Veszély: függőség kialakulása:

http://www.boldog-gyermek.hu/internetfuggoseg_teszt.html



Mire használhatjuk az internetet?

1. Tanulás, ismeretszerzés

- a) Keresés az interneten keresőprogramok segítségével pl.: Google.
- b) Wikipédia használata.
- c) Oktatóvideók keresése pl.: YouTube oldalon.

<https://www.youtube.com>

2. Kommunikáció, kapcsolattartás

- a) Elektronikus levelezés.
- b) Közösségi hálózatok.
- c) Csevegő programok, chat.
- d) Online fórumok.

3. Új lehetőségek, véleménynyilvánítás

- a) Kommentek, megosztások.

4. Szórakozás

- a) Rádióadók, tévé csatornák adásainak online elérése, régebbi műsorok visszanezése.
- b) Videómegosztó oldalak.
- c) Filmek letöltése.
- d) Játékkonzolok használata.
- e) Internetes játékok – ezek gyakran kéretlenül, akár böngészés közben jelennek meg. Fontos megtanítani, hogy mire figyeljen a gyerek mielőtt bármire rákattint:
 - Kell-e regisztrálni? Milyen adatokat kell megadni?
 - Videokamera aktív-e a játék során?
 - Pénzbe kerül-e?
 - Más játékosokkal (idegenekkel) kapcsolatba kerül-e a játék során?

Beszéljünk őszintén az Internet veszélyeiről is!

Legfontosabb, hogy gyermekünk megkapja tőlünk azt az odafigyelést, ami az élet más területén is jár neki. Ha sikerült kialakítanunk egy stabil bizalmi kapcsolatot, ez hozzájárul ahhoz is, hogy az interneten nagyobb biztonságban legyen. Teljesen biztonságos internet nincs, de megtaníthatjuk a legfontosabb szabályokat, megtaníthatjuk azt, hogyan jelezzék, ha baj van.



1. Az ismerkedés veszélyei

Sohasem tudhatjuk, hogy az újonnan megismert „barát” tényleg az-e, akinek mondja magát (neme, kora, hobbijai ...)

Intő jelek:

- Nincsenek kommentek a képei alatt.
- Alig van ismerőse, követője.
- Nincsenek közös képei az osztálytársaival.
- Bizalmas dolgokat mond el magáról és azokról érdeklődik.
- Túlságosan kedves, hízelgős.
- Személyesen akar találkozni.

Óvintézkedések:

- A közösségi oldal profil beállítása legyen privát (a felhasználó dönti el, ki láthatja).
- Csak a személyes ismerősöket igazoljuk vissza. Az ismerősök listája ne legyen látható.
- Ismerjük meg, és tartsuk be a közösségi oldal által ajánlott biztonsági előírásokat.
- Interneten megismert „baráttal” kiskorú gyermek ne találkozzon egyedül.

2. Kamu oldalak, álhírek az interneten

Ma már minden kicsit is gyakorlott felhasználó létre hozhat saját weboldalt vagy indíthat blogot. Ez azzal a veszéllyel is jár, hogy megszorodtak azok az oldalak, amik álhírek terjesztésére szakosodtak. Céljuk az internet használók megtévesztése, befolyásolása, manipulálása. Magunk is hozzájárulhatunk ezen álhírek terjesztéséhez, ha pl. megosztjuk a Facebookon.

Hogyan dönthetjük el, hogy egy hír igaz-e vagy hogy egy oldal hiteles-e?

Néhány szabály:

- Ha valami nagyon hihetetlennek tűnik, az általában az is pl. csodaszerekről szóló hírek, amik fiatalítanak, fogyasztanak vagy éppen gyógyítják a rákot.
- Gyanús, ha nincs feltüntetve a cikk szerzője.
- Gyanús, ha valamit lájkolni kell ahhoz, hogy megnézhessek.
- Gyanakodjunk akkor is, ha az oldal neve nagyon hasonlít közismert hiteles oldalak nevére vagy ha rákeresünk az oldalra nem kapunk találatot.
- Érdeemes megnézni a kamu oldalak aktuális listáját

3. Ami az internetre kikerült, annak örökre nyoma marad

Az online világban tett cselekedeteinknek ugyan olyan következményei lehetnek, mintha a valós világban tettük volna. Egy sértő bejegyzés törlése nem oldja meg a problémát, attól, hogy nem látjuk, az már felkerült az internetre, „önálló életet él”, nem tudjuk visszafordítani.

Mire ügyeljünk?

- Kerüljük a meggondolatlan, első felindulásból tett bejegyzéseket, kommenteket.
- A feltöltött képekkel mások visszaélhetnek, megváltoztathatják - még a megosztás előtt gondolkodjunk.
- 18 év alatti személyről készült meztelen (félmeztelen is!) kép vagy video gyermekpornográfiának minősül, a megosztása és a saját eszközön való tárolása bűncselekmény!
- Saját magáról készült és továbbküldött kép azt is bajba sodorja, akinek a gépén megtalálják.
- Fontos figyelmeztetni a gyerekeket, hogy olyan felvételt még a szerelmével se osszon meg, ami büntetőjogi felelősséget von maga után.

4. Online zaklatás (cyberbullying), erőszak az interneten

„Az internetes zaklatás alatt azt értjük, amikor sorozatosan és hosszabb ideig fennálló szándékos sérelem okozás áldozatává válik egy tinédzser az interneten vagy mobilon. Lehet ennek célja a fiatal megalázása, fenyegetése, nevetségessé tétele, kiközösítése, lejáratása, negatív színben feltüntetése.”¹

Az online térben a gyerekek gyakran nem kímélik egymást, igazi adok-kapok zajlik, ahol az elkövető sokszor egyben áldozat is. Sok esetben a zaklató nem érzi úgy, hogy amit tett bántó a másik fél számára. A kölcsönös bizalmon alapuló szülő-gyermek kapcsolat ilyen esetekben is sokat segít. Érezze a gyermek a szülő támogatását akkor is, ha butaságot csinált.

Hogyan előzhető meg?

- Tudatosítsuk a gyermekekben, hogy az online térben leírt bántó szó ugyanúgy fáj, mint a szemtől szembe mondott. A küldés gomb megnyomása előtt gondolja át még egyszer, hogy egy vagy két nap elteltével is ugyanazt írná-e? A dühös emberek olyat is megtesznek, amit egyébként nem tennének.
- Ne továbbítson, ne osszon meg olyan dolgot, amiből később baja lehet.

¹ <https://www.kek-vonal.hu/index.php/hu/szolgalattasok/internetbiztonsag/395-internetes-zaklatas>

- Ha olyan képet, videót tölt fel, amin más is szerepel, az összes szereplő hozzájárulása szükséges. Gyerekről csak a szülő hozzájárulása után lehet nyilvánosan posztolni.
- Módosult tudatállapotban semmit ne tegyen ki az internetre, józanul könnyen megbánhatja.



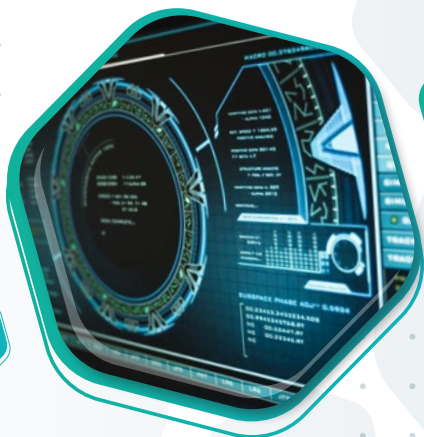
5. Az internetes vásárlás veszélyei

A webáruházakban való vásárlást egyre többen részesítik előnyben, mert gyors és kényelmes, határok nélküli, óriási a kínálat. Csalókkal azonban itt is találkozhatunk, sok bosszúságtól kímélhetjük meg magunkat, ha körültekintően vásárlunk és erre tanítjuk gyermekeinket is.

- Érdemes leellenőrizni a weboldalt, ahonnan vásárolni szeretnénk, gyakoriak a hamis oldalak.
- Bankok, pénzintézetek soha nem kérnek adatokat e-mailben.
- Ismeretlen feladótól érkező e-mailben szereplő linkre nem szabad rákattintani.
- Netbankos fizetés esetén kérjük sms vagy token szolgáltatást a tranzakcióról.
- Ha más is használja a számítógépet nem szerencsés, ha engedjük a böngészőnek, hogy megjegyezze a jelszavainkat.
- Érdemes tisztában lenni az internetes vásárlásra (e-mailben, telefonon leadott rendelések, teleshop) vonatkozó fogyasztóvédelmi szabályokkal.

6. Vírusok és kémprogramok

Minden internethez kapcsolódó számítógép ki van téve a számítógépes vírusok, kémprogramok, hackerek támadásainak. 100%-os védelem sajnos nem létezik, de minimálisra csökkenthetjük a fenyegetettséget vírusirtó programok használatával, megfelelően beállított tűzfalal. Fontos, hogy az adott program legfrissebb verziója fusson a gépünkön.





7. Életkornak nem megfelelő tartalmak

Böngészés közben előfordulhat, hogy a gyerekek felnőtteknek szóló oldalakra bukkannak. Fontos felvilágosítani őket mi az amire kattinthatnak és mi az amire nem. Jó, ha tudnak arról, hogy az interneten, a játékokban, közösségi oldalakon elérhetőek alkohol- és kábítószerfogyasztást, dohányzást népszerűsítő, vagy pornográf tartalmak. Az ilyen tartalmak akkor igazán veszélyesek, ha gyermek nem tudja kivel megbeszélni. Léteznek olyan szűrők, amelyek nem százszázalékosan, de védenek az ilyen tartalmak ellen.

8. Felnőttek veszélyeztető magatartása

Sok szülő előszeretettel oszt meg gyermekéről készült felvételeket a közösségi oldalán. A jogszabályok szerint minden gyermeknek joga van véleményt nyilvánítani az őt érintő ügyekben. Így arról is dönthet hogy milyen képek, videók kerüljenek ki róla az internetre.

Érdeemes pár dologra figyelünk:

- Posztolás előtt nézzük meg a beállításinkat. Kik fogják látni?
- Más gyerekéről nem posztolhatunk képet.
- Saját gyermekünkről ne tegyünk ki meztelen fotót, gondoljunk arra, mit fog szólni pár év múlva, ha nagyobb lesz.
- Ügyeljünk a lakásban készült fotókra, értéktárgyaink ne legyenek láthatók.

Programok, melyeket a gyerekeink használnak

I. Közösségimédia-oldalak

1. Facebook

Egyik legnagyobb közösségi hálózat:

- Bejegyzéseket, képeket, hozzászólásokat tehetünk közzé.
- Privát üzeneteket küldhetünk.
- Egyes dolgokat online meg lehet vásárolni.
- Sértő, veszélyes tartalmakat be lehet jelenteni a „Bejelentés” menüpont alatt.
- 13 éves kor alatt zártkörű adatlapot hoz létre.

2. Instagram

Az Instagram egy közösségi hálózat, amely fényképek és rövid videók okostelefonon történő megosztásán alapul. A felhasználók fényképeket és videókat tölthetnek fel, amelyeket különböző művészi hatású effektekkel/szűrőkkel láthatnak el, feliratozhatják, beállíthatják a készítés helyét, majd ezt követően megoszthatják másokkal. A felhasználó követői kedvelhetik a képet, videót és hozzá is szólhatnak.

3. Snapchat

A Snapchat 12 évesnél idősebb felhasználóknak szól. A Snapchat felhasználói által küldött fényképek és videók a

megtekintésüket követő 10 másodpercen belül törlődnek, ezért népszerű az alkalmazás. A felhasználók úgy gondolják, hogy a képeiket nem lehet elmenteni, vagy tovább küldeni, de fontos tudni, hogy a Snapchat-képek nem tűnnek el teljesen a felhasználó eszközéről.

4. TikTok

Egy IOS és Android rendszereken elérhető alkalmazás, amelyre a felhasználók rövid, zenés, táncos, tátogós vagy tréfás videókat tölthetnek fel, és megnézhetik mások tartalmait.

Magyarországon nagyon sok gyerek erre a közösségi-média-platformra regisztrál először, akár már 9-10 éves korában.

A népszerű felhasználókat, TikTok-sztárokat több millióan követik, de a többséget csak a saját barátaik; a legtöbb felhasználó maga is tölt fel tartalmat.



A TikTok divattrendekre és kihívásokra fókuszál; ugyanarra a témára sokan készítenek videókat.

5. Twitch

A Twitch egy olyan platform, ahol élő közvetítéseket lehet sugározni (vagyis „streamelni”), illetve nézni. Fő területe a videójáték, az e-sport, a podcast, de zene és talkshow is megjelenik a felületen. Böngészőben és mobilalkalmazáson keresztül is elérhető.

A hasonló érdeklődési körrel rendelkezők egymásra találhatnak: közös rajongás, közös téma, közös személyiség – közösségi érzet kialakítása.

6. Discord

A Discord egy VoIP alkalmazás amit elsősorban játékosok számára fejlesztettek (azért, hogy játék közben tudjanak egymással beszélgetni), de például a digitális munkarend során is használják kommunikációs felületként. Szöveges és hangalapú, illetve videós kommunikációra is alkalmas, valamint képeket, emojikat is lehet a platformon küldeni. A moderátori rendszer segíti a tartalomszűrést.

II. Azonnali üzenetküldő alkalmazások

1. WhatsApp

A Whatsapp egy VoIP mobilalkalmazás, üzenetküldő szolgáltatás, amellyel online ingyenesen tudunk szövegeket küldeni, hanghívást indítani, illetve videocsetelni, akár csoportos beszélgetéseket indítani. Sokféle eszközön és platformon elérhető, Android, iOS és Windows operációs rendszeren is fut.

2. Viber

A Viber a fiatalabb korosztály egyik első okostelefonos alkalmazása, a korhatár ellenére már 9-10 éves kortól használják, gyakran osztálycsoportokban is. Az azonosítás a telefonszámunkkal történik, jelszót a Viber generál. A Viberen a kortárs online zaklatás egyik gyakori formája a csoportból való kizárás, de a gúnyolódás más formái is megjelennek. Az üzenetek elrejtésének, törlésének lehetősége megnehezíti a visszakövetést.

3. Messenger

A Facebook ingyenes üzenetküldő szolgáltatása, amely okoseszköztől és számítógépről egyaránt elérhető. Kiválóan alkalmas szöveg, kép, videó küldésére, valamint több résztvevős videóhívásra is a „Szobák” funkció segítségével. A csoportos hívásban közös videónézésre is lehetőség van. A Messenger alkalmas fájlok küldésére is. A magánszféra és a személyes adatok védelmében érdemes a helymegosztást kikapcsolni.



III. Játékok

1. Fortnite

Sokszereplős online akciójáték, legnépszerűbb játékmódja az úgynevezett „Battle Royale”, vagy-is „mindenki-mindenki ellen”. Erőszakmentes módja a „Party Royale”.

A játék úgy kezdődik, hogy legfeljebb 100 játékost „dobnak le” egy szigetre. A harchoz szükséges fegyvereket és egyéb eszközöket a játék során a „térképen” elhelyezett pontokon szedik fel. A játék rendkívül gyorsan fejlődik, minden évadban számos újdonságot tartalmaz.

A rajzfilm-jellegű karakterek, a játék vizuális világa miatt a fiatalabbak számára is vonzó. A Fortnite játékmechanizmusa kifejezetten épít arra, hogy a játékosoknak „muszáj” legyen beszerezni az új kellékeket. Ezért gyermekek számára nem javasolt a fizetés engedélyezése

2. PUBG

APUBG egy kompetitív, többszereplős katonai stílusú akciójáték, „Battle Royale”: 100 játékos játszik egymás ellen, hogy a végén az utolsó győzzön. A játék során eszközöket lehet gyűjteni, és elpusztítani az ellenfeleket. Felkavaró elemek, erőszak a játékban előfordulhat. A játék kommunikációs hangvétele az agresszió, zaklatás vagy kéretlen kapcsolatfelvétel terepe is lehet. Itt is jellemző a „kikényszerített” alkalmazáson belüli vásárlás.



3. Roblox

A játék egyfajta „digitális homokozó”, a szabad, szabályok nélküli játék terepe. A felhasználók „mikrojátékokat” fejlesztenek, amelyeket egymással is megosztanak. A játékosok kiélhetik kreativitásukat, közösen is játszható a barátokkal. A regisztráció ingyenes, de megjelennek játékon belüli vásárlások.

4. Brawl Stars

Brawl Stars sokszereplős online, valós idejű stratégiai akciójáték, amelyben a játékosok, egyénileg vagy csapatban csatákat vívnak. A játék legfőbb vonzereje, hogy nagyon sok játékmódot használ. A játékban van kapcsolattartási lehetőség: a játékosok a belső csetfelületen kommunikálnak. Fejleszti a stratégiai tervező képességet, a csapatban való együttműködést.

IV. Gyermekek számára nem ajánlott anonim üzenetküldők

1. Ask.fm

Olyan közösségi webhely, ahol a felhasználók megválaszolják ismerősök és idegenek kérdéseit. Nem kell nevet megadni, ezért a kérdések többnyire olyanok, amelyeket személyesen nem szívesen tennének fel. Szinte minden téma előfordulhat.

2. Anotalk

Az AnoTalk egy gyermekek számára egyáltalán nem ajánlott, ellenőrizhetetlen platform, ahol nagy eséllyel lehet explicit, pornográf tartalmakkal találkozni. A regisztráció és az adatok ellenőrzésének a hiánya visszaélésekre, hamis személyiség felvételére adhat lehetőséget. Teljesen sosem lehetünk biztosak abban, hogy hány éves, és milyen nemű a beszélgetőpartnerünk valójában. (Hasonló a **Chat Alternative** is.)

3. Tellonym

A Tellonym anonim üzenetküldő alkalmazás, amelyben böngészőben és mobilalkalmazásként is elérhető. Követhetünk más felhasználókat, akiknek kérdéseket lehet feltenni. A profilok nyilvánosak, tehát nem kell ismerősnek lenni ahhoz, hogy lássuk egy felhasználó kérdéseit és válaszait.

A felhasználók névvel vagy névtelenül kérdéseket küldenek más felhasználók számára, akik megválaszolhatják azt. A kérdés csak akkor jelenik meg látható módon a fogadó fél falán, ha megválaszolta azt. Az anonimitást kihasználva sokan arra használják az alkalmazást, hogy sértő vagy megszegényítő üzeneteket küldjenek a többi felhasználónak, ez pedig könnyen online zaklatáshoz vezethet.



V. Egyéb platformok, alkalmazások

1. Reddit

A Reddit egy olyan ingyenesen használható közösségi weboldal, ahol a felhasználók különböző cikkeket, híreket, képeket és videókat oszthatnak meg másokkal, a lehető legkülönbözőbb témakörökben. A fiatalok felhasználókát semmilyen tartalomszűrés nem védi, noha a felnőtt tartalmak jelezve vannak, a káromkodás nincs a felnőtt tartalmak köré sorolva.

2. Tumblr

Egy mikroblog platform. Felületén rövid terjedelmű szövegeket, illetve képet, videót, GIF-animációt vagy hangfelvételt lehet megosztani. A bejegyzések újraoszthatóak, a szöveg terjedelme legfeljebb 475 karakter lehet.

Az Instagramhoz vagy a Twitterhez hasonlóan (amelyekre a legjobban hasonlít), a Tumblr-ön is követni lehet az általunk kedvelt oldalakat. A többi, online kommunikációra alkalmas felülethez hasonlóan itt is megjelenhet az online zaklatás, a behálózás, kéretlen kapcsolatfelvétel.

3. Tinder

A 17 év felettieknek szánt Tinder adatvédelmi szabályzata

13 évnél idősebb gyermekek számára is lehetővé teszi, hogy regisztráljanak, és felveszék a kapcsolatot a közelükben tartózkodókkal. A randialkalmazásként ismert Tinder profilképei között is bőven akad nem gyerekeknek való. A fiatalabb felhasználók szüleinek tudniuk kell, hogy a Tinder földrajzi helymeghatározási és anonimitási jellemzői lehetőséget biztosíthatnak a zaklatásra (mert használatakor látszik, hogy hol van éppen a felhasználó).



KÖZÖSSÉGI MÉDIA ÉS INTERNET

korhatárok

12

Flickr*

13

Facebook, Instagram, Snapchat,
Whatsapp, Youtube, Pinterest, Twitter,
Google+, Tumblr, iTunes, Skype,
Minecraft, LinkedIn, Foursquare

14

Spotify*

17

Xbox live**

18

Playstation
network**,
Tinder, Netflix

*hozzáférés az összes funkcióhoz
17 vagy 18 éves kortól

**önálló hozzáférés,
szülői fiók nélkül

Ajánlott weboldalak:

- <https://privacy.thewaltdisneycompany.com/hu/biztonsagos-internethasznalat/>
- www.biztonsagosinternet.hu
- www.kek-vonal.hu
- www.saferinternet.hu
- www.yelon.hu
- www.hipersuli.hu

Forrás:

- Telenor – Hogyan beszéljünk a gyerekekkel az internetről? című kiadvány
- <https://digitalisgyermekvedelem.hu/platformok>
- Fotók forrása: pixabay.com, pexels.com, freepik.com

SZÉCHENYI
2020

Kiadó:

Szentes – Nagytemplomi Református Egyházközség

2021.



MAGYARORSZÁG
KORMÁNYA

Európai Unió
Európai Szociális
Alap



BEFEKTETÉS A JÖVŐBE