Az internet veszélyei házi feladatok

Tartalomjegyzék

A fiatalokat fenyegető veszélyek az interneten

Bukva Bence

Internetes zaklatás

A köztudatban az internet a pedofil emberek fő vadászterülete. A valóságban azonban az azonos életkorú fiatalok között történik a zaklatások legnagyobb része. A molesztálás illetve a ráerőszakolt kapcsolatok száma viszonylag alacsony, bár sosem lehet tökéletes pontossággal felmérni őket, hiszen lehetséges hogy az áldozat nem akar róla beszélni, titkolja, hogy zaklatják.

A pedofilok képesek beleolvadni a névtelen online közösségekbe, célszerű óvatosnak lenni, nem kell elhinni mindent amit az interneten lát az ember, illetve javasolt megbízható oldalakat látogatni. Megtiltani az internetet nem lehet, hiszen a pozitívumai túlteszik a negatívumait, ezért érdemes felállítani egy szabályrendszert.

A zaklatást az interneten is olyan emberek hajtják végre, mint akik ezt az utcán is tennék. Az erőszakos környezetben felnövő ember az interneten éli ki az agresszivitását, mit ahogy a mondás tartja ,, Mások nyomora kioltja a miénket".

Az áldozat gyakran tudja hogy ki zaklatja őt, hiszen főképp az iskolai összetűzések nyomán indulnak el az úgynevezett "bosszúhadjáratok". A szülők ilyenkor valószínűleg nem tud semmit, hiszen a gyerek próbál egyedül túljutni ezeken az eseményeken, illetve a szülők nem veszik olyan komolyan a virtuális világot, mint a fiatalok. Ha fizikailag bántanák a gyereket, azt a szülők észre tudnák venni, azonban a lelki sérelmeket amit az internetről hoznak a gyerekek, a szülők nem tudják felfedezni. Az ilyen sérelmek kezelésére jött létre több szervezet is, azonban a tinédzserek először a barátaikkal beszélik meg a bajaikat, kevesebbszer a szüleikkel és legutolsó esetben, ha már minden kötél szakad, akkor veszik fel a kapcsolatot ilyen szervezetekkel.

Mit lehet a zaklatás ellen tenni?

A probléma csökkentését egy olyan felnőttel lehet elérni, aki a gyerek környezetében van és érzelmileg támogatja és segíti a gyereket, illetve átlátja a problémáit. A szülőnek figyelemmel kell kísérnie, hogy a gyerek mit csinál a szabadidejében, ha internetezik milyen oldalakat látogat, mit tölt le vagy mit tölt fel, vagy kikkel tartja a kapcsolatot és fel kell világosítania gyerekét arról , hogy milyen veszélyek leselkednek rá. Manapság már nem ritkák az olyan programok, melyek korlátozzák a gyerek hozzáférését a digitális világhoz. Ehhez azonban szükséges, hogy a szülő rendelkezzen valamennyi számítástechnikai tudással is.

Kutatások szerint a magyar fiatalok naivabbak, mint a nyugat európai társaik, szóval több személyes adatot adnak meg magukról.

Az internetes visszaélések bővítik az erőszak amúgy is nagy eszköztárát, és ezen esetben az elkövetők az internet anonimitása miatt nagyon ritkán jutnak a rendőrsége kezére. Nem lehet megmondani a probléma nagyságát, mivel ritkán derülnek ki az ilyen esetek.

Cyberbullying

A cyberbullying első ismertebb példája a kanadai Ghyslain Raza esete. Ghyslain 2002-ben filmre vette ahogy egy partvisnyéllel utánozni próbálta a Star Wars filmek jedi lovagjait. Ghyslain egy 15 éves, túlsúlyos gyerek volt, így a mozdulatai viccesnek találtattak a megtekintők közt. Az osztálytársai, megtalálván a videót, feltették azt az internetre, s ők maguk sem számítottak rá, hogy milyen népszerűségnek fog az örvendeni. Telt az idő, és észrevették, hogy hatalmas mennyiségű ember töltötte le a felvételt. Ghyslain egy netes mémmé nőtt (mém= egy olyan dolog ami divatszerűen terjed az interneten), s még honlap is készült, ahová az eredeti videó és a viccesen megszerkesztett változatai is felkerültek. Az oldalt 2 év alatt 900 millió ember kereste fel. Sajnos az amúgy is önértékelési problémákkal küzdő Ghyslain megaláztatásként fogta fel a hírnevét, s emiatt többször iskolát váltott és pszichiátriai segítségre szorult.

A cyberbullying, Ghyslain esete jól mutatja, egy olyan zaklatásfajta, amit szándékosan többször megismételnek az internet segítségével. A zaklatók élhetnek az e-mail, online felületek, közösségi oldalak adta lehetőségekkel. Az agresszió különféle módokon jelenhet meg: kiközösítés, identitásrablás, fenyegető e-mailek, rosszindulatú pletykák, vagy akár olyan információt is közölhet a zaklató, amit az áldozat nem akar a nyilvánosság elé tárni. Ismeretlen emberek is becsatlakozhatnak a zaklató táborába, csak azért, hogy szórakoztassák magukat, mert viccesnek találják a helyzetet.

A nagy internetes vállalatok a személyes információk alapján címzik nekünk a reklámokat, s ezekből a reklámokból élnek, így érdekük, hogy minél több személyes adatot tároljanak el. Ennek is köszönhető, hogy a magánélet kezd egyre csökkeni az internet világában. Vannak akik tudtuk nélkül teszik ki magukat a cyberbullyknak azzal, hogy közzéteszik életük eseményeit, és bele sem gondolnak, hogy mi lesz hogyha az információ rossz kezekbe kerül.

A hagyományos zaklatás és a cyberbullying között nagy az átfedés, de új kiváltott hatásai is vannak, érzelmileg megterhelőbb mint az ódivatú formája.

A cyberbullying-ot egy amerikai ügyvédnő, Parry Aftab szerint három cselekvési módon lehet kivédeni. Először hagyják abba amit csinálnak, akár e-mailről van szó, akár chatelésről. Ezután használják a blokkolás funkciót, ami általában az internetes szolgáltatásnál elérhető, a zaklatók ellen tervezve. Végül mondják el a szülőnek mi történt velük. A szülők ilyenkor nehéz helyzetben vannak, hiszen feltehetőleg ők sincsenek a helyzet magaslatán, mivel kevésbé ismerik ezt a világot. Egy szó mint száz, az internetes zaklatás ellen a leghatásosabb védekezés a megelőzés

Források:

http://www.kamaszpanasz.hu/hirek/szuloknek/4161/internetes-zaklatas

http://www.mipszi.hu/cikk/110104-elektronikus-zaklatas-cyberbullying

A fiatalokat fenyegető veszélyek az interneten

Danó Dániel

Manapság a korombeli fiatalok, velem egyetemben idejük nagy részét az interneten lógva töltik. Ezt nagymértékben megkönnyítette az okostelefonok megjelenése, ami lehetővé tette, hogy majdnem mindenhonnan fel tudjunk csatlakozni a világhálóra. Ez igen megkönnyíti a mindennapi életet, mivel olyan gyorsan és egyszerűen jutunk hozzá a szükséges információkhoz, abban a pillanatban, amikor kellenek, mint még soha.

Viszont ez, hogy körülbelül bármit megtalálhatunk hihetetlenül könnyen, az internetes keresők segítségével, nem kifejezetten veszélytelen. Persze, egy tapasztalt embert, főleg felnőttet jóval kevesebb veszély fenyeget, de ez egy 10 év körüli gyerekről, aki a számítógép előtt ül, és egyedül játszik, nem mondható el. Játék és netezés közben olyan oldalakra kerülhet teljesen véletlen, ami igen káros lehet a lelkére nézve. Már ha csak a hírportálokat nézzük, olyan, eredetileg csak nagykorúaknak szánt fotókat láthat, például egy katasztrófa sújtott területen készült, akár halottakat ábrázoló képet, ami egy ilyen fiatal gyereket nagyon felkavar. És az egyetlen „óvintézkedés”az, hogy nem közvetlen az oldalra irányít a link, hanem először feltesz egy kérdést, hogy elmúltunk-e már 18 évesek. Ha elképzelünk egy 10 éves gyereket, amint ezt a kérdést látja, szinte magunk előtt láthatjuk az kíváncsiságtól egyre izgatottabb arcát. Természetes, hogy 18 év felettinek jelöli magát, hogy láthassa a kívánt oldalt, így minden akadály nélkül láthatja a káros tartalmat. De ez persze más, felnőtt tartalmú weboldalra is igaz. Egy kis kattintgatás és a gyerek máris olyan helyre jut, ahova nem kellett volna.

Az ilyen véletlenből amellett, hogy olyat láthat a kis felhasználó, amit nem kéne, sok más dolog veszélye is fennáll. Bizonyos oldalak hozzáférést kérhetnek a felhasználó bizonyos adataihoz, mint például telefonszámok, lakcím. Ezeket egy kisebb gyerek, egy esetleges regisztráció során magától is meg tudja adni, és ha ezt egy szülő felügyelete nélkül teszi, ezek az adatok rossz kezekbe kerülhetnek. Ez később nagy kárt okozhat a család számára, ha esetleg egy olyan emberhez kerül, aki visszaélhet velük. Telefon és bankkártya-számok segítségével pénzt tudnak leemelni az emberek számlájáról és átutalni a sajátjukra. Ezt kifejezetten internetes fizetésre tervezett kártyákkal lehet kivédeni. Ezekre a külön bankkártyákra mindig kisebb címleteket lehet átutalni és nem köthető a nagyobb pénzösszegeket tartalmazó kártyákhoz, így elkerülhető, hogy nagyobb mennyiségű pénz tűnjön el váratlanul.

A közösségi oldalak megjelenése is újabb veszélyforrásokat eredményezett. Még a legnagyobb, biztonságosnak gondolt oldalak is, mint a Facebookon,

megvannak a maguk lehetőségei az ember rosszakaróinak számára. A regisztrálásnál a legtöbb ilyen oldal elkéri az ember bizonyos adatait. Általában eldönthetjük, bizonyos korlátok közt, hogy mennyit adunk meg, de van néhány alapkérdés, ahol meg kell adni az e-mail címet, nevet és nemet. Gyakran az ember telefonszámát is kéri, de ezt nem feltétlen kell megadni. A közösségi oldalak lényege ugye, hogy ismerőseinket megtaláljuk és üzeneteket és információkat közöljünk velük. Viszont ha nem teszünk meg néhány alap óvintézkedést, akkor sok dolgot megláthatnak ismerőseink ismerősei, amit már nem feltétlen jó. Ez arra is igaz, ha ismeretlen embereket jelölünk vissza. Ezek azért veszélyesek, mivel nem ismerjük ezeket az idegeneket és nem tudhatjuk miért érdeklődnek irántunk. Elég egy-két képet feltenni és máris tudják, hol járunk, kikkel barátkozunk és mik a szokásaink. Innentől nem nehéz egy betörést megszervezni, csupán figyelni kell az ember posztjait. Elég, ha felkerül egy kép, a családi hétvégéről vagy nyaralásról, az egy jelzésként szól a betörőknek, hogy itt az idő a cselekvésre. Szinte mi magunk biztosítottunk nekik a lehetőséget és információkat mindehhez.

Az interneten való ismerkedés másik nagy veszélye, hogy nem ismerjük az emberek valódi énjét. Látott gesztusok hiányában nem lehet tudni a szavak mögötti őszinteséget. Bármilyennek mondhatják magukat, mi nem tudhatjuk igazat beszélnek-e. Hazudhatnak korukról, szándékukról és jellemükről. Neten keresztül szóba elegyedhetnek fiatal gyerekekkel. Találkozót nem nehéz megszervezni, és ha már sikerült elcsábítani valahova, onnantól az erősebb felnőtt bármit meg tud tenni. Ez tökéletes lehetőség a gyerekrablók és pedofilok számára.

De nem kell ilyen komolyan megszervezett bűncselekménynek lennie egy találkozónak ahhoz, hogy rossz vége legyen. Mint már említettem, a közösségi oldalakon keresztül nehéz kiismerni az embert. Ha egy lány félreismer egy fiút, aki megtetszett neki a neten, szívesen találkozik vele. És így lehet, hogy a randi nem pont úgy alakul, ahogy a másik fél tervezte és ezért elkezdhet erőszakoskodni.

Mostanság már ajánlott odafigyelni, hogy miket postolunk ki az üzenőfalunkra. Vigyázni kell, mert az emberek bírálhatnak minket értük és commentjeink miatt. Kétszer is érdemes átgondolni, mielőtt leírjuk. Sőt, ha nem vigyázunk, megeshet, hogy később látjuk kárát meggondolatlanságunknak. Dönthet úgy az egyetem, vagy a kiszemelt munkaadó, hogy ők nem szeretnék

hírnevüket olyan munkatárssal rontani, aki az interneten például trágár módon viselkedik, esetleg rasszista megjegyzései vannak.

Ha internetet használunk, nagyon oda kell figyelni mindenre, mivel rengeteg lehetőség van arra, hogy valamilyen módon kárt szenvedjünk. A fiatalabbaknak szükségük van egy bizonyos szülői felügyeletre, nehogy nagy bajt okozzanak tapasztalatlanságukkal és azzal, hogy nincsenek tisztában tettük súlyosságával.

Átverések az interneten

Gál Eszter

Az internet nagyon sok változást hozott a mindennapi életünkbe. Könnyebb lett a kapcsolattartás, könnyebben és gyorsabban jutunk hozzá az új, minket érdeklő információkhoz. Ma már vásárolni, állást keresni is tudunk az interneten, azonban nem árt vigyázni, hiszen könnyen csalók áldozataivá válhatunk. Hogyan ismerhetjük fel a csalókat, az álprofilokat és mit tehetünk ilyenkor?

Mivel az internetet rengeteg ember használja, a bűnözők ezen a területen is megtalálhatóak és próbálják a gyanútlan, tapasztalatlan, vagy jóhiszemű emberek pénzét kicsalni. Az internet ideális terep a svindlereknek, hiszen itt arc és név nélkül is az emberek bizalmába férkőzhetnek. Az internetes csalásoknak rengeteg fajtája van, és természetesen itt is mindig újabb átverések jelennek meg.

Az internetes csalások egyik igen elterjedt fajtája a nigériai típusú levél átverés. Az ilyen átverések elkövetői többnyire Afrikából küldözgetnek rossz angolsággal megírt e-maileket. Ezekben, az e-mailekben az elkövetők általában egy magas rangú tisztviselőnek adják ki magukat, és segítséget kérnek ahhoz, hogy egy nagyobb értéket, leginkább készpénzt megmentsenek az állam vagy rokonaik elől. Előfordul az is, hogy az illető valutát akar váltani, persze feltűnően kedvező arányban és mennyiségben. Az átverés trükkje az, hogy a címzett csak a személyes adatai megadásával juthat hozzá a mesebeli összeghez. A csalók a megszerzett adatok segítségéven könnyen el tudják tulajdonítani a címzettek pénzét a bankkártyáikról. Ennek a fajta átverésnek létezik egy rosszabb fajtája is. Ebben az embereket az e-mailekben arra próbálják meg rávenni, hogy vegyenek részt egy üzleti találkozón egy fejlődő országban. Az áldozatok ezzel teljesen kiszolgáltatják magukat a bűnözőknek. Az ilyen találkozókon nem ritka a zsarolás és a fizikai erőszak sem. Az internetes átverés e fajtája onnan kapta a nevét, hogy a Nigéria bűntető törvénykönyv külön foglalkozik az ilyen típusú csalásokkal, mivel ez az ország ötödik legfontosabb bevételi forrásává vált. A nigériai kormány kitart amellett, hogy mindent megtesznek az ilyen fajta bűnözés ellen, azonban nemzetközi becslések szerint akár 50-100 ezer ember is foglalkozhat ezzel Nigériában. Ugyanezen az elven működik a „holland lottó”. Az áldozatok e-mailt kapnak arról, hogy megnyerték általában a holland lottó főnyereményét és a pénzt meg is kapják, ha felhívnak egy számot és megadják a csatolt azonosítót. Csupán annyit kell tennie, hogy előre kifizeti a nemzetközi adókat. Nagyon sok ember a csalók áldozatává vált, amikor kifizette az adót, ám a nyeremény összegét sosem látta. Ebben az esetben

a svindlerek ugyan kisebb összeghez jutnak hozzá, mint a nigériai leveleknél, azonban ennek a csalásnak több áldozata volt.

Nagyon sok csaló célja a banki adatok megszerzése. Sokan ezt úgy próbálja elérni, hogy a címzettek bankja nevében írnak e-mailt. Az ilyen átveréseket nevezzük adathalászatnak, nemzetközi nevén pishingnek. A csalók a bank nevében az ügyfél e-mail címének megerősítését kérik, amihez csupán egy linkre kell kattintani. Az ügyfél így egy álweblapra jut, amely a logók és a bank által is használt betűtípus miatt nagyon hasonlítanak a bank hivatalos oldalához. Itt a banki adatok megadását kérik tőle az azonosításhoz. Ez után az áldozatokat megnyugtatják, hogy az azonosítás megtörtént és átirányítják őket a bank hivatalos honlapjára, azonban már a csalók kezében vannak az adatik. Fontos tudni, hogy a bankok ilyen jellegű adatokat sosem kérnek e-mailben, pontosan a biztonság miatt.

Az internetes átverések talán az online kereskedelem körül a legelterjedtebbek. Sokan hamisított termékeket kínálnak jóval kedvezőbb áron, sokan álprofilokról próbálnak nem létező dolgokat eladni. Az ilyen álprofiloknak gyakran vannak pozitív értékelési, amelyeket maga az elkövető készít, hogy könnyebben megtévessze a vásárlókat. Az ilyen csalások esetében a csalók előleget vagy a teljes összeg kifizetését kérik még mielőtt átadnák a megvásárolni kívánt dolgot és eltűnnek a pénzzel. Az aukciós oldalakon az eladók nagyobb része valóban tisztességes és valóban olcsóbban hozzá lehet jutni a kívánt dolgokhoz. Az ilyen átveréseket legkönnyebben úgy lehet elkerülni, ha személyesen fizetünk és vesszük át, amit vásároltunk.

Az átverések egy viszonylag új fajtája, hogy a számítógépen egy üzenetablak jelenik meg, azzal a szöveggel, hogy a rendőrség vagy egy másik hatóság blokkolta a felhasználó PC-jét, mivel olyan fájlt töltött le, amivel szerzői jogot sértett vagy tiltott tartalmat tekintett meg. Az általában rossz magyarsággal megírt üzenet szerint egy bizonyos pénzösszeg átutalásával a megadott számlaszámra, adott időn belül a blokkolás feloldható. A rendőrség sosem zárolja senki számítógépét internetes rendszeren keresztül és az is elég gyanús, hogy pár ezer forinttal meg lehet úszni egy büntetőeljárást, mégis ilyen típusú csalásoknál is sokan, akik nem is tettek semmi törvénytelent, kifizetik a kért összeget, mivel a hatóságok nevével, logóival élnek vissza és büntetőeljárással fenyegetnek.

Vannak olyan bűzözők is, akik az együttérzésre, szimpátiára hatva próbálnak e-mailben adományokat kérni általában beteg, éhező gyerekeknek. Az adományt egy számlaszámra kell elutalni, azonban a segítség sosem jut el a rászorulókhoz. Fontos, hogy ha adakozni akarunk győződjünk meg róla, hogy valóban az az intézmény vagy szervezet gyűjti az adományt, amelyet segíteni szeretnénk, és ne egy e-mailben álló számlaszámra utaljuk a pénzt. Szintén az érzelmekre épít a romantikus átverés, melynek során a csaló virtuális kapcsolatot alakít ki, később akár házasságot is ígér. Ehhez azonban különböző költségekre hivatkozva pénzt kér az áldozatától. A csaló egy álprofilt hoz létre, amelyen kitalált adatokat ad meg, és általában egy kevésbé ismert modell képét használja. Pár hónap virtuális kapcsolat után a kitalált személy valamilyen baleset vagy őt ért kellemetlenség miatt pénzt kér kölcsön. A csalás mindaddig tart, amíg az áldozat hajlandó fizetni, utána a csaló eltűnik. Az áldozat a szégyenérzete miatt általában nem is jelenti a csalást, mivel önmagukat hibáztatják.

Az internetes csalások áldozatainak túlnyomó többsége nem jelenti a csalást, mivel önmagát hibáztatja érte, vagy úgy ítéli meg, hogy a tőle kicsalt pénzösszeg túl kicsi ahhoz, hogy a rendőrség érdemben foglalkozzon vele. Mivel a legtöbb elkövető ellen, akik kisebb csalásokat hajtanak végre, nyomozás sem indul, ezért a csalók száma igen magas. Fontos, hogy az emberek ne higgyenek el mindent, ne adják meg a legfontosabb adataikat online és legyenek körültekintőek ha olyan ajánlatot kapnak egy ismeretlentől, ami hihetetlenül jól hangzik vagy ha éppen az együttérzésükre akarnak hatni.

Források:

http://lopasesatveres.network.hu/blog/lopas_es_atveres_klub_hirei/hogyan_vedekezzunk_az_internetes_atveresek_ellen

http://lopasesatveres.network.hu/blog/lopas_es_atveres_klub_hirei/internetes-csalasok-csalo-alszereto-halojaban-vagyis-a-romantikus-atveres

http://www.magyarefk.hu/sajtoszoba-hirek/204-ujabb-csalasi-formak-es-atveresek-az-internetes-kereskedelembenszukseges-az-ovatossag.html

Mobileszközök védelme

Horváth Péter

A mobiltelefonok olyan készülékek, amelyek képesek vezeték nélkül beszéddel vagy más módon kommunikálni. Megjelenésükkor még csak hanghívás funkcióval rendelkeztek, majd a mobiltelefon gyártó cégek versengése miatt újabb és újabb funkciókkal és alkalmazásokkal (SMS, e-mail, internet, WAP, MMS, tévé, videokamera, napló, fényképezőgép, rádió, naptár és mp3) bővültek. A kétezres évek vége felé a mobiltelefonok új generációja jelent meg. Az okostelefonok nagy mértékben hasonlítanak egy leegyszerűsített, miniatűr számítógéphez, ami telefonként is képes működni. Áruk a gyártó cég, a beépített funkciók és alkalmazások függvényében eléggé magas, akár a több százezer forintot is elérheti, ám értékcsökkenésük a többi elektromos készülékhez hasonlóan szintén drasztikusan nagyon gyors. Ennek oka a mobiltelefon gyártó cégek versengése. Egyre több és újabb modellt dobnak a piacra, melyek újabb és újabb funkciókkal rendelkeznek, ezért a másfél-két éves készülékek már elavultnak számítanak.

Mobiltelefon elvesztése vagy elhagyása esetén a teendők

Ma egy felgyorsult világban élünk. Az embereknek egyszerre több dologra kell figyelniük, mint amire képesek, ezért sokszor átsiklunk olyan dolgok fölött, mint például az, hogy hova tettük le a mobiltelefonunkat. Az elveszített telefont szerencsés esetben a megtaláló visszajuttatja a gazdájához, rosszabb esetben ellopja. A tolvajok is elég gyakran lopnak mobiltelefont. Erre az esetre ajánlott a PIN-kód beállítása. Ha a készülék lemerül, vagy a tolvaj kikapcsolja csak három próbálkozása lesz beütni a kódot, és elég nagy a valószínűsége, hogy nem találja el a helyes számsorozatot. Ezután a telefon a PUK-kódot kéri, melyet a tolvaj szintén nem ismerhet és ezt csak a mobilszolgáltató ügyfélszolgálata árulhatja el a készülék tulajdoni papírjainak a bemutatásakor. A mai okostelefonokon már be lehet állítani egy számkódot vagy feloldómintát, amivel meg lehet védeni még a személyes adatokat is. Ha a telefon képernyőzára leidőzít, a tolvaj nem fér hozzá a mobiltelefonon lévő alkalmazásokhoz, adatokhoz. A mobilszolgáltatóknál le lehet tiltatni a SIM kártyát, így a tolvaj nem tudja telefonálásra használni a készüléket. Lopás esetén le lehet tiltani a mobiltelefont is. Először a mobilszolgáltatónál kell jelenteni a telefon eltűnését, utána be kell nyújtani egy kérelmet a telefon letiltásáról. Ehhez az eljáráshoz szükséges a mobiltelefon megvételét igazoló számlák bemutatása és a kérelemben a készülék IMEI számának feltüntetése. A leghatékonyabb megoldás, a mobiltelefon eltűnésének a bejelentése a szolgáltatónál. A bejelentést követően a szolgáltató folyamatosan figyeli az ellopott készüléket, így ha a tolvaj használatba veszi a telefont (telefonál, SMS-t küld) a szolgáltató be tudja mérni a használat pontos helyét és riaszthatja a rendőrséget.

Mobiltelefonok lehallgatása

Az egész világon hatalmas problémát jelent a mobiltelefonok lehallgatása. A mobiltelefon használók mindössze négy százaléka védekezik valamilyen módon a lehallgatás ellen és ebből körülbelül fél százalékuk lehallgatás biztos. A hagyományos telefonok egyáltalán nem védhetők lehallgatás ellen. Csak az okostelefonokra lehet letölteni olyan alkalmazást, ami megvédi a telefonon tárolt adatokat, azonban hanghívások és SMS-ek ellen szinte védetlenek az emberek. Minden telefonba elmentett adatot ellophatnak, vagy minden hanghívást rögzíteni tudnak. Persze ez az emberek nagy részének nem jelent gondot. Elsősorban a nagyszámú ügyfél adatait kezelő pénzügyi szolgáltatók, a jelentős tulajdonnal és saját fejlesztéssel rendelkező technológiai, ipari vállalatok, a média és a tömegek számára értékes hírekkel szolgáló ismert emberek számára jelenthetnek veszélyt ezek a lehallgatások. Persze akár kisebb cégek és vállalkozások számára is veszélyt rejtenek a hackerek. Meglehetősen nagy anyagi károkat okozhat az óvatlanság.

Vírusok

A mobiltelefonok egyre kifinomultabb eszközök, melyek főként a használóik kényelmét szolgálják. A mobiltelefonra írt alkalmazások fejlesztésével párhuzamosan sajnos a vírusírók is egyre több vírusprogramot fejlesztenek, amelyek komoly károkat okozhatnak a felhasználók készülékében. Manapság nagyon precíz vírusokat írnak, amelyek emeltdíjas SMS-eket küldenek, képeket és egyéb vírusokat, kártevőket töltenek le. Vagy akár bluetooth-on keresztül más eszközöket is megfertőzhetnek. Létezik olyan vírusprogram is amely távirányítást biztosít a vírus írójának a ”fertőzött” készülék felett. A mai telefonokba már gyárilag be van építve néhány vírusirtó program, amelyek megakadályozzák a vírusok telepítését. Fontos az elővigyázatosság, inkább a kockázatmentes módszereket érdemes követni. Vírusirtó programok óriási választékából lehet válogatni az Android és IOS alapú készülékekre egyaránt. Nagy részük ingyenes, persze van néhány, amelyek egy fél szendvics árába, pár száz forintba kerülnek. Ezeket szinte mindenki megengedheti magának. Csak hivatalos, megbízható forrásból töltsünk le képeket, zenéket, alkalmazásokat vagy játékokat. Ajánlott csak az adott operációs rendszerhez tartozó helyről (Google play, Apple store) letölteni az alkalmazásokat, mert ott általában előre ellenőrzik az programokat. Ám mindenki elkövethet hibát. Az emelt díjas hívások és SMS-ek letiltásával is sok pénzt lehet spórolni, ha véletlen elszabadulna egy vírus a készüléken. A programok telepítése előtt fontos átgondolni, hogy tényleg szükséges-e letöltenünk. Egy nem telepített program nem okozhat gondot. Egy program telepítésekor gondosan olvassuk el a hozzá tartozó leírást és legyünk gyanakvóak, ha egy játék vagy zene letöltő alkalmazás olyan erőforrásokat kér, amelyek nem

szükségesek a működéséhez. Lehetőleg ne hagyjuk bekapcsolva a bluetooth vagy infra kapcsolatokat, ha már nem használjuk őket, mert sokban megkönnyítik a vírusok települését. Csak akkor kapcsoljuk be ezeket az alkalmazásokat, mikor ténylegesen is használjuk őket. Ha véletlen mégis ”elkapnánk” egy vírust, forduljunk szakemberhez minél hamarabb, és ne próbáljuk meg egyedül eltávolítani.

Forrás:

http://www.telenor.hu/ugyfelszolgalat/feltoltokartya/help

http://www.lopotttelefon.hu/

http://www.lopotttelefon.hu/az-elvesztett-mobil-telefonokkal-kapcsolatos-teendok/

http://www.telenor.hu/ugyintezes/tudnivalok/adatmodositas/letiltas

http://hu.wikipedia.org/wiki/Okostelefon

http://hu.wikipedia.org/wiki/Mobiltelefon

http://hvg.hu/tudomany/20140217_majdnem_minden_mobil_lehallgathato/

http://fn.hir24.hu/penzugy/2014/02/17/vigyazzon-gyerekjatek-lehallgatni-a-mobiljat/

http://nol.hu/gazdasag/okostelefonok__alig_vedekezunk_a_lehallgatas_ellen-1445217

http://www.virushirado.hu/mobilvirusok

http://www.itkommando.hu/site/a_halozat_szolgalataban/tanulmanyok/mobileszkozok-vedelme/

Tárgymutató