Biztonságtudatosság az informatikaoktatásban

Csubák Dániel[1], Kiss Attila[2],

[1]csuby@caesar.elte.hu
ELTE IK, Információs Rendszerek Tanszék
[2]kiss@inf.elte.hu
ELTE IK, Információs Rendszerek Tanszék

Absztrakt. Gyermekeink felé gyakran elhangzik a tanács, hogy ne bízzanak idegenekben, ne fogadjanak el semmit idegenektől, mi magunk pedig előfordul, hogy valamiről azt gondoljuk, hogy az túl jól hangzik ahhoz, hogy igaz legyen, ezeket a tanácsokat azonban mégsem követi mindenki, amikor a kibertérben történő aktivitását folytatja. Az előadás tisztázza a mindennapokban használatos informatikai védelem eléréséhez szükséges fogalmakat, javallatokat, ellenérveket és bevált módszereket mutat be, hogy az informatikai eszközök használata során előforduló, az Internet helytelen használata és a kártékony felhasználók által jelentett valós veszélyre hívja fel a figyelmet. Az elhangzó javallatok egy olyan rést fednek be, mely az informatika oktatásának biztonságtudatos viselkedésre ösztönző részét érinti. Az előadásban érintett témák: kiberbiztonság alapjai; anonimitás az Interneten; személyes adatok védelme; jelszavak; webes biztonság alapjai; kiemelten veszélyeztetett személyek (pl.: gyerekek, időskorúak); biztonság a szociális hálózatokon; mobileszközök biztonsága.

Kulcsszavak: informatikai biztonság, biztonságtudatosság, szociális hálózatok biztonsága, okoseszközök biztonsága, webes biztonság

1. Bevezetés

Az információs társadalom életének rengeteg területén egyre több számítógép, illetve internethez való kapcsolódási képességgel rendelkező eszköz jelent meg, mely a számos előny mellett különféle veszélyforrásokat is magában hordoz. Az internetkapcsolattal rendelkező okoseszközök számának robbanásszerű növekedése azonban nem vonta maga után az emberi gondolkodásmódbeli változást, a biztonságtudatosabb hozzáállást.

A kibertér megannyi előnye mellett számos veszélyt rejt az óvatlan felhasználók számára, mely az egyszerű adathalászattól kezdve a személyes identitás eltulajdonításáig bármi lehet. A tanulmány célja, hogy megismertesse az olvasót a veszélyekkel, felhívja a figyelmét arra, hogyan védekezhet az esetleges támadások ellen, és mindemellett tudatosítsa benne, hogy szemléletváltásra van szükség, mely az informatikai eszközök felhasználásának, illetve az informatika oktatásának biztonságtudatos viselkedésre ösztönző részét érinti.

A továbbiakban a 2. fejezet megismerteti az olvasót a kiberbiztonság alapvető fogalmaival, majd a 3. fejezet a helyes jelszóválasztás szükségességét indokolja, és olyan irányelveket prezentál, mely ebben segítségünkre lehet. A 4. fejezet több alfejezeten keresztül vezeti be az olvasót a webes biztonságba, kitérve az Internet publikusságára, és arra, hogy mit kell szem előtt tartanunk, mielőtt bármit online publikálnánk, tisztázza az anonimitás kérdését, és megismerteti az olvasót két fontos böngészés közbeni témával, a tanúsítványokkal, illetve az aktív tartalmakkal. Az 5. fejezet a szociális hálózatok használata közben felmerülő biztonsági kérdéseket járja körbe, míg a 6. fejezet a mobileszközök használata során történő elővigyázatossági irányelveket prezentál. A 7. fejezetben kitérünk a kiemelten veszélyeztetett személyek, különös tekintettel a gyermekek esetére, majd a 8. fejezetben összefoglaljuk munkánkat.

A tanulmány készítéséhez a szerzők az U.S. Department of Homeland Security[1] US-CERT[2] osztálya által kiadott anyagokat tekintették irányadó példának, ezeket részletesen az irodalomjegyzékben mutatják be.

2. A kiberbiztonság alapjai

Manapság életünk jelentős része a számítógépek, okoseszközök és az Internet használatával zajlik – használjuk a kommunikációhoz, szórakozáshoz, utazáshoz, vásárláshoz, az egészségügyben és különféle kritikus infrastruktúrákban, emellett személyes adataink egy részét online tároljuk, így mindezek sebezhetővé, támadhatóvá válnak, amennyiben nem vagyunk kellőképpen elővigyázatosak. A kiberbiztonság célja, hogy megelőzéssel, észleléssel és reakciókkal válaszoljon az ezen területeket is érintő támadásokra. A sokrétű felhasználás mellett a veszélyforrások is legalább ennyire sokszínűek, mind erősségüket, mind céljukat tekintve – léteznek vírusok, melyek káros tartalmat propagálhatnak ismerőseinknek online kommunikációs csatornáinkat használva, de a támadó célja az is lehet, hogy megszerezze bankkártya adatainkat, hogy ezzel vásárlásokat hajthasson végre. Emellett fájljaink kompromittációján túl elképzelhető, hogy egy támadás során eszközünk felett az irányítást megszerezvén a támadó azt további bűncselekményekhez kívánja felhasználni. Mindezek ellen tudunk védekezni, fontos azonban tisztázni, hogy nem létezik 100%-os védelem, de a bemutatott lépések, módszerek segítségünkre lehetnek abban, hogy minimalizáljuk az áldozattá válás kockázatát.

Az alapvető fogalmakat tekintve *hackernek* vagy *támadónak* nevezzük azon személyeket, akik szoftver-, vagy rendszergyengeségeket használnak ki saját érdekükben. Szándékaik nem minden esetben károsak számunkra, így az eredmény is változatos skálán mozoghat. *Rosszindulatú kód*, vagy *malware* olyan kategóriát jelöl, mely magában foglal minden forráskódot, melynek célja a számítógépünk, rendszerünk támadása lehet. Ezen kód különböző jellemzőkkel rendelkezhet, így lehet, hogy felhasználói interakciót igényel a lefutása, mielőtt megfertőzné a számítógépünket (például egy email csatolmányának megnyitása, vagy egy weboldal megtekintése), de előfordulhat, hogy szoftversebezhetőséget kihasználva erre nincsen szüksége, vagy álcázhatja magát számunkra hasznos programnak, és kecsegtető ígéretekkel vehet rá minket arra, hogy lefuttassuk. Rosszindulatú kódra jó példának tekinthetőek a különféle *vírusok* és *férgek*. *Sebezhetőségnek* olyan szoftverhibákat nevezünk, melyeket a támadók kihasználva megfertőzhetik, kompromittálhatják eszközünket, rendszerünket (például HeartBleed, ShellShock). A sebezhetőségek ellen a legjobb védekezés a szoftvereink folyamatos frissítése, *biztonsági frissítések* telepítése. [1]

3. Jelszavak

A jelszavak manapság az autentikáció (azonosítás) legalapvetőbb formáját képzik, gyakran csak ezek alapján kapcsolják össze a felhasználókat személyes információikkal. Nap mint nap használjuk őket, például amikor bankkártyánkkal fizetünk, pénzt veszünk fel, bejelentkezünk számítógépünkre, vagy valamilyen online fiókunkba. Észben tartásuk bonyolult, felesleges dolognak tűnhet, hiszen miért akarná egy támadó pont a mi fiókjainkat feltörni, amikor látszólag semmi értékes információ nincs benne – azonban ez a hozzáállás téves, tekintsük csak példának a kü-

[1] Az Amerikai Egyesült Államok Nemzetbiztonsági Hivatala

[2] United States Computer Emergency Readiness Team (US-CERT)

lönféle elektronikus ügyintézési folyamatokat, ahol szenzitív adatainkat, vagy az azokhoz történő hozzáférés kulcsát mind email fiókunkban tároljuk.

A helyes jelszóválasztás kritikus fontosságú privát adataink védelmének érdekében. A támadók különféle gépi, illetve heurisztikus eszközöket használhatnak arra, hogy jelszavunkat kitalálják, azonban a lentebbi stratégiák segítségünkre lehetnek, hogy ennek kockázatát csökkentsük. A támadásokat tekintve a legáltalánosabb módszerek a brute-force, mely esetében a támadó próbálgatással, az összes lehetőség kipróbálásával igyekszik megtalálni jelszavunkat, mely ellen a legtöbb bejelentkezésért felelős motor valamilyen szintű védelmet nyújt számunkra, például három sikertelen próbálkozás után egy captcha-t oldat meg velünk. A szótárazáson alapuló támadások, melyek azon esetekben veszélyesek, ha jelszavunk a szótárban megtalálható szavakat tartalmazza.

A fentiekből látszik, hogy a szótárazás ellen úgy tudunk védekezni, ha jelszavunk nem tartalmaz szótári szavakat, a brute force támadás legjobb ellenszere pedig a hosszú, bonyolult jelszavakban rejlik. Az alábbi irányelvek segíthetnek a jó jelszóválasztásban:

- Jelszavunkban ne használjunk könnyen kitalálható személyes információt, melyet a támadó akár online is megtalálhat. Például valamely hozzátartozónk neve a születési évszámával pont ezen okból nem megfelelő.
- Lehetőleg ne használjunk szótári szavakat.
- Alakítsunk ki egy emlékezést segítő mondatot, melyet használva könnyebben megjegyezhetjük a komplex jelszavakat. Például a „Darth Vader a kedvenc főgonoszom” mondat alapján könnyen emlékezhetünk az ebből képzett jelszóra, mely „DVakf” lehetne.
- Jelszavunkban használjunk kis- és nagybetűket, számokat és speciális karaktereket. A korábbi példát továbbgondolva, jelszavunk lehetne „DV4kf!”.
- Ha van lehetőségünk fontoljuk meg a jelmondatok alkalmazását. Ezek általában hosszabb mondatok, melyeket a megfelelő módon kiegészítve speciális karakterekkel, erős jelszót kapunk. Ügyeljünk arra, hogy ezen mondat ne tartalmazzon könnyen felismerhető mintát például dalszövegből vagy idézetből.
- Minden rendszerhez más jelszót használjunk. Ez tovább hátráltatja a támadót, hiszen ha megszerezte egyik jelszavunkat, azzal csak egyik fiókunkhoz és nem minden adatunkhoz fog tudni hozzáférni.

A megfelelő jelszó kiválasztásával még nem végeztünk. Mindez után ügyelnünk kell arra, hogy jelszavunkat ne hagyjuk könnyen elérhető helyen, azt ne tudják megszerezni tőlünk saját gondatlanságunk, vagy nem megfelelő eszközhasználat miatt. Léteznek olyan eszközök, melyek megjegyzik jelszavainkat, ezek kiválasztásánál ügyeljünk arra, hogy a szoftver a jelszavakat titkosított formátumban tárolja. [2]

4. Webes biztonság alapjai

Az Internet manapság általánosan használt erőforrás, rengeteg információ lelhető fel segítségével, azonban vannak irányelvek, melyeket szem előtt kell tartanunk, ha biztonságosan szeretnénk használni.

4.1. Az internet publikussága

Az Internet használata során sosem szabad elfelejtenünk, hogy az általánosságban véve publikus. Amint valami felkerül az Internetre, csak nagyon nehezen, vagy sehogy sem tudjuk az adott információt eltüntetni onnan, hiszen például a keresőmotorok gyorsítótáraikban azt eltárolhatják.

Sokan azt feltételezik, hogy különösebb elővigyázatossági lépések nélkül is anonim módon böngésznek, azonban ez a hozzáállás téves, hiszen bárki ugyanolyan egyszerűen találhat meg minket az Interneten, ahogyan azt mi is viszont megtehetjük.

Adatok publikálása, online elérhetővé tétele során tartsuk szem előtt, hogy csak olyasmit osszunk meg, aminek az esetében nem zavar minket az, ha széles körben elérhető lesz. Írjunk bár blogot, készítsünk weboldalt, tisztában kell lennünk azzal, hogy azt ezentúl olyan emberek is meg fogják találni, akiket nem ismerünk, sosem találkoztunk velük, vagy az eredetitől eltérő céllal szeretnék az általunk publikáltakat felhasználni. Természetesen léteznek módszerek, hogy online adataink elérhetőségét korlátozzuk, azonban ezek változatos biztonságot kínálnak. Legyünk körültekintőek azzal kapcsolatban, hogy mit tárunk a nyilvánosság elé, hiszen egy elérhető email cím megnövelheti a spam üzeneteink számát, amennyiben pedig szenzitív adatokat osztunk meg publikusan, azzal könnyen adathalászat áldozataivá válhatunk. [3]

4.2. Anonimitás az Interneten

Sokakban él a feltételezés, hogy böngészés közben anonim az Interneten, ez természetesen téves, hiszen minden egyes online akciónknak marad valamilyen nyoma, lépten-nyomon információt gyűjtenek rólunk különféle céllal. Ezen információk között lehetnek például az alábbiak:

- IP cím, mellyel minden internetre kapcsolódó számítógép rendelkezik. Ezen cím általában egyedi (léteznek kivételek, például egy router mögötti alhálózat gépei kifelé ugyanazt a címet használják) és alkalmas arra, hogy azonosítson minket. Léteznek módszerek, melyek segítségével elfedhetjük címünket, ilyen például a különféle proxy-, vagy anonimitást biztosító szolgáltatások használata, azonban ezek is csak bizonyos mértékű használat után adnak teljes anonimitást. Az IP cím alapján következtetni lehet az internetszolgáltatónkra és jó eséllyel lokációnkra is. Amennyiben kíváncsiak vagyunk arra, hogy csupán IP címünk alapján mennyi információ deríthető ki rólunk, a [4] web oldal lehet a segítségünkre.
- Domain név, mely csoportokat jelöl, és az Interneten minden ezen csoportok valamelyikébe tartozik. Legegyszerűbb példa az URL-ek végén található domain jelzés (magyar oldalak esetén többnyire .hu).
- Böngészésben érintett szoftvereink minőségét, milyenségét, verzióját is meg lehet határozni, amennyiben erre lehetőséget biztosítunk. Könnyen gondolhatnánk, hogy kit érdekel mindez, mire megy valaki azzal, ha ezt tudja, de ez a hozzáállás ismét téves. Ha például elfelejtettünk biztonsági frissítéseket telepíteni, és a böngésző egy korábbi, hibás verzióját használjuk, ennyi adat már elég a támadónak ahhoz, hogy tudja, milyen szoftversebezhetőséget kell kihasználnia ahhoz, hogy kártékony tevékenységet folytathasson számítógépünkön.
- Oldalfelkeresések alatt azt értjük, hogy könnyedén gyűjthető információ arról, hogy mely oldalakon mennyit tartózkodtunk, hogyan jutottunk oda, stb.

Az ilyen módon összegyűjtött információ változatos célokra használható fel. Elképzelhető, hogy a szolgáltatók csak monitorozzák oldaluk látogatottságát, de lehetséges, hogy egy hacker gyűjt éppen potenciális áldozatokat azzal, hogy tevékenységüket megfigyeli. Manapság a legtöbb böngészőben beállítható, hogy milyen preferenciákkal rendelkezünk azt illetően, hogy mely adatainkat adja ki a böngésző olyan oldalak számára, melyek ezt igénylik. Ezen beállításokat mindig tüzetesen nézzük át, és igyekezzünk a lehető legminimálisabb információt szolgáltatni magunkról. [5]

4.3. Tanúsítványok weboldalakon

Amennyiben egy weboldal garantálni szeretné biztonságunkat, adatainkat pedig titkosított csatornán szeretné bekérni, szüksége van hozzá egy tanúsítványra. ennek meglétét két módon tudjuk ellenőrizni:

- A böngészőben – implementációtól függően, de általában az url mez előtt – megjelenik egy lezárt lakat ikon.
- A weboldal url-je http:// helyett https://-el kezdődik.

Ez annyit jelent, hogy egy tanúsítványkibocsájtási jogkörrel rendelkező hatóság biztosít minket arról, hogy az adott weboldal kihez tartozik, milyen tevékenységet űz. Amennyiben a fentieknek megfelelő weboldalt tekintünk meg a böngészőnk automatikusan ellenőrzi annak tanúsítványát. Ahhoz, hogy ezt effektíven hajthassa végre fontos, hogy mindig telepítsük a böngészőnk legújabb biztonsági frissítéseit, hiszen ezek tartalmazzák a nem megbízható tanúsítványok, vagy az esetlegesen kompromittálódott hatóságok listáját (utóbbi nagyon ritka, de meglehetősen kellemetlen esemény, mivel ez azt jelenti, hogy az összes, az adott hatóság által aláírt tanúsítvány kompromittálódott, nem megbízható). Ekkor először megvizsgálja, hogy a tanúsítvány érvényes-e, valóban annak a részére szól-e, aki számára kibocsájtották, és a hatóság, mely aláírta azt, megbízható-e. Abban az esetben, ha böngésző ebben problémát talál, azt általában egy – ismét implementációtól függően – figyelemfelkeltő ablakban közli velünk, ahol leírja az észlelt problémát, és ránk bízza a döntést, hogy a kockázat ellenére szeretnénk-e használni a weboldalt. Ebben az esetben figyeljünk arra, hogy a megtekintéssel járó biztonsági kivételt a böngészőnkkel ne tároltassuk el, hiszen ha a weboldal mégsem megbízható, adataink olyan résztvevők kezébe is juthatnak, ami nekünk nem állt szándékunkban.

A tanúsítványokban történő bizalom annyit tesz, hogy megbízunk abban a hatóságban, aki ezt aláírta a tulajdonosa számára. Olyan ez, mint egy erkölcsi bizonyítvány weboldalak, szolgáltatások számára, ahol egy megbízható harmadik fél voksol amellett, hogy az adott tanúsítvány tulajdonosa az, aki. Léteznek más elven működő tanúsítványok is, melyek esetében a hitelesítés folyamata máshogy működik, azonban a bizalmi lánc ezen esetekben is megvan.

Ha magunk szeretnénk megvizsgálni egy tanúsítványt – mert például a böngészőnk egy adott oldalt nem talált biztonságosnak, de mi valamiért mégis bíznánk benne – az alábbiakra érdemes odafigyelnünk:

- Ki írta alá a tanúsítványt? Ebben az esetben megbízható hatóságot kell keresnünk. Ezek listája publikus (Magyarországon ilyenek például a Közigazgatási Gyökér Hitelesítés-Szolgáltató (KGyHSz), NetLock, Microsec).
- Ki számára írták alá a tanúsítványt? Az oldal valóban a kedvezményezett tulajdonát képezi-e?
- Mikor jár le a tanúsítvány? A legtöbb tanúsítványt 1-2 évre írják alá (tanúsítványkiadó hatóságok esetén ez 10 év körül lehet). Egy lejárt tanúsítvány jelenthet feledékenységet, de az esetek nagyobb részében lehetséges, hogy inkább bizalmi kérdésről van szó. Amikor túl hosszú időre kibocsájtott tanúsítványokat látunk, kezdjünk el gyanakodni azok érvényességét, megbízhatóságát illetően. [6]

4.4. Aktív tartalmak és cookie-k

Sokak számára böngészés közben a design, vagy egy-egy funkció működésének mögöttes értelme mágiával egyenértékű, meg sem próbálják azt megérteni. Ezen hozzáállás hibás, hiszen a

funkcionalitásbeli javulás sok esetben különféle mértékű kockázattal jár együtt, melynek megértése fontos lehet az Internet biztonságos használatának szempontjából.

Az aktív tartalmak alatt olyan forráskódot, scriptet, vagy futtatható programot értünk, mely valamelyest kiterjeszti az egyszerű HTML funkcionalitását, illetve eszköztárát, hogy az jobban nézzen ki, elláthasson más feladatokat is. Sajnálatos módon ezen funkcionalitás azonban használható kártékony módon is, ezt pedig a támadók előszeretettel használják ki, hogy rosszindulatú weboldalakra irányítsanak minket, vagy nem kívánt tartalmakat töltessenek le velünk.

A két leginkább ismert, elterjedt és népszerű aktív tartalom a következő:

JavaScript, mely mára széles körben, majd minden oldal által használt script nyelv. Népszerűsége funkcionalitása mellett abban is rejlik, hogy a felhasználók már megszokták a kinézetet és a kényelmet, melyet biztosítani tud számukra, azonban pont ebben rejlik a veszélye is, hiszen a támadók manipulálhatják ezen kódot úgy, hogy a felhasználót például rosszindulatú oldalra továbbítsa.

Java és ActiveX vezérlők, melyek kész programokat jelentenek, melyek letölthetőek, vagy a böngészőből futtathatóak. Ezek funkciótára meglehetősen széleskörű, de a kockázat is legalább ekkora lehet, hiszen amennyiben egy támadó által kezelt tartalmat futtatunk, az lényegében bármit meg tud tenni számítógépünkön, amit a nem kártékony programnak megengedtünk.

Természetesen az aktív tartalmak nem mind károsak, azonban meglehetősen népszerű eszközök a támadók kezében. Amennyiben olyan weboldalt böngészünk, melyben nem teljesen bízunk meg, gondolkodjunk el az aktív tartalmak blokkolásán. Ez csökkentheti az oldal funkcionalitását számunkra, azonban jelentősen növelheti online biztonságunkat.

Böngészés közben a böngésző, a különféle weboldalak információt tárolnak el rólunk, melynek egyik megszokott módja a cookie-k használata. A cookie-k tartalmukat és élettartamukat tekintve több félék is lehetnek:

- Session cookies: csak addig vannak érvényben, amíg a böngészőt használjuk, amint azt bezárjuk, törlődnek. Általában az oldalakon történő navigációban, hitelesítéskor vannak segítségünkre.
- Perzisztens cookies: személyes preferenciáinktól függően hosszabb időre tárolja el őket a böngésző. Céljuk, hogy a megszokott kinézetet, default beállításokat (például alapértelmezett email fiók) a látogatott oldal meg tudja jegyezni.

A fentebbiekből látható, hogy amennyiben ezen cookie-kat valaki meg tudja szerezni, ellophatja adatainkat, szélsőséges esetben néhány weboldalra vonatkozó identitásunkat is. Léteznek módszerek, melyeket az oldalak tulajdonosai kikényszeríthetnek (például https kommunikáció, biztonságos, titkosított cookie-k használata, stb.), ezek növelhetik biztonságunkat és csökkenthetik a sikeres támadás kockázatát. Emellett a böngészőnk – implementációtól függően – információt tud szolgáltatni számunkra az eltárolt cookie-król, melyek alapján azok biztonságosságát el tudjuk dönteni. Amit nem szabad elfelejtenünk, az annyi, hogy ha nem megbízható, vagy publikus számítógépet használunk, töröljük böngészésünk nyomait, így a cookie-kat is, hogy más felhasználók abból ne tudjanak rólunk adatokat kinyerni. Ebben segítségünkre lehet a legtöbb böngészőben elérhető inkognitó böngészési mód, mely nevével ellentétben nem biztosít online anonimitást, de nem tárolja el adatainkat, preferenciáinkat. [7]

5. Biztonság a szociális hálózatokon

A különféle szociális hálózatok használata napjainkban egyre inkább elterjedt. 2015-ös adatok szerint [8] a vezető Facebook közel másfél milliárd felhasználóval rendelkezik, míg a Twitter

átlépte a félmilliárd felhasználós küszöböt, a LinkedIn pedig a 400 milliósat. Átlagosan az emberiség 29%-a használ szociális hálózatokat, és a fejlett országok tekintetében ez a szám még jelentősebb, illetve a felhasználók közel két harmada okoseszközökről is használja mindezt.

A szociális hálózatokat a felhasználók különféle célokra használják, melyek között a kapcsolattartás legalább annyira fontos, mint a munkakeresés, vagy éppen a zenehallgatás, véleménykifejtés. Egyes hálózatok más-más speciális területekre fókuszálnak, így az általános Facebook-tól kezdve tekinthetjük a Twittert, ami egy jó megfogalmazás szerint lassan az „Internet SMS-e" lesz, vagy a LinkedIn-t, mely munkakeresésben, szakmai kapcsolatok építésében lehet segítségünkre, míg a MySpace-n zenei ízlésünket és egyéb szórakoztatásban számunkra fontos dolgokat hirdethetünk.

Természetesen az egyre növekvő felhasználószám magával vonja azt a tényt is, hogy a támadók figyelme egyre inkább a szociális hálózatok felé fordul. Ezek használata során a következő általános veszélyekkel kell tisztában lennünk:

- A támadók a szociális hálózatokat arra használhatják, hogy vírusokat terjesszenek el. Ezek lehetnek egyszerű URL-ek, valamilyen általános üzenettel egy ismerősünktől, melyre rákattintva a mi fiókunk is fertőzötté válik, és továbbterjeszti a vírust. Mindig járjunk el körültekintően, mielőtt gyanús hiperhivatkozásra (hyperlink) kattintunk. Az alábbi ábra megfelelően szemlélteti, hogy hogyan tudjuk beazonosítani a kéretlen, esetleg káros tartalmakat.

1. ábra: Megbízható és hamis hyperlinkek videótartalmat ígérnek a Facebook-on [forrás: http://techchai.com/wp-content/uploads/2011/03/253193289.png].

- Különféle eszközök, például hamis applikációk használatával a támadók részlegesen, vagy teljesen átvehetik az irányítást fiókunk felett, melyet például arra használhatnak, hogy általunk propagáljanak kártékony tartalmat, melyre ismerőseink bennünk megbízva rákattintanak. Mindig tekintsük meg, hogy egy-egy alkalmazás mihez kér hozzáférést, és gondoljuk át, hogy milyen jogokat adunk azoknak. A látszólag indokolatlanul tartalommegosztási jogot kérő applikációk használatát lehetőleg mellőzzük.
- Kártékony felhasználók a „social engineering" módszereit használva próbálhatnak minket meggyőzni arról, hogy olyan oldalra navigáljunk, mely rosszindulatú kódot propagál. Ezen

támadások esetén a hacker önmagát megbízható félnek adja ki, ezzel próbál minket rávenni, hogy hibát kövessünk el. Amikor kérdés merül fel egy-egy tartalommegosztó identitását illetően, mindig győződjünk meg arról, hogy az illető az-e, aminek vagy akinek mondja magát. A legtöbb szociális hálózat társít hivatalos oldalakat médiaszereplőkhöz, ezen oldalak ellenőrzöttek és megbízhatóak, így ez segítségünkre lehet a döntésben. A 2. ábra szemlélteti ennek a megjelenését a Facebook-on.

2. ábra: Ellenőrzött oldal a Facebook-on [forrás https://facebook.com].

- Amennyiben óvatlanul sok információt teszünk nyilvánossá a szociális hálózatokon, támadók képesek lehetnek arra, hogy identitásunkat ellopják, az összegyűjtött adatok alapján eljátszanak minket akár online, akár valós formában. Mindkét eset rendkívül veszélyes, ezért gondoljuk át, hogy mit osztunk meg magunkról ezeken a platformokon.

Általános irányelvnek tekinthető, hogy a szociális hálózatok használata során legyünk elővigyázatosak, gondoljuk át, milyen adatokat osztunk meg magunkról. Amennyiben ezzel kapcsolatban kétség merül fel bennünk, képzeljük el, hogy az Internetre történő kiírás helyett az adott információt a homlokunkra írjuk fel, és bárki, aki velünk szembe jön az utcán, ezt láthatja, letörölni pedig csak nehézségek árán, fáradtságos munkával tudjuk majd. Tüzetesen vizsgáljuk meg biztonsági beállításainkat, hiszen a legtöbb szociális hálózat lehetőséget kínál nekünk arra, hogy beállítsuk, mely tartalmakat kik láthatják profilunkon. Osszunk meg minél kevesebb információt a publikummal, korlátozzuk a megosztott adatok jó részét ismerőseinkre! Kerüljük el a gyanús, nem megerősített, nem hitelesített forrásokból származó applikációk használatát! [9][10]

6. Mobileszközök biztonsága

A különféle okoseszközök használatának elterjedésével ezek biztonságára is különös figyelmet kell fordítanunk. Ezen eszközök közös jellemzője, hogy könnyen hordozhatóak, kis helyen elférnek, de ez az előnyük különféle biztonsági kockázatokat rejt magában.

Amennyiben hordozható eszközünket eltulajdonítják, az első, szembetűnő ellopott dolog maga az eszköz lesz. Azonban ennél többről van szó, hiszen az eszközt rendszeresen különféle feladatok elvégzésére használjuk, adataink egy részét azon tároljuk. Tisztában kell lennünk azzal, hogy a kockázat mértéke a tárolt információk mennyisége és fontossága függvényébennövekszik és azzal is, hogy a különféle okoseszközeink hozzá vannak kapcsolva egyes fiókjainkhoz, így az ügyes tolvaj ezekhez is hozzáférhet.

Amennyiben biztosítani szeretnénk eszközeinket, az alábbi irányadó elveket érdemes követnünk:

- Mindenképpen védjük jelszóval az eszközt. Ez egy laptop esetén magától értetődik, egy okoseszköz esetében pedig a biztonsági beállítások között választható.
- Ügyeljünk ezen eszközökre ugyanúgy, mint más értéktárgyainkra, hiszen még ha maga az eszköz nem is minden esetben képvisel egy drágább ékszerrel összemérhető értéket, a rajta tárolt adatok függvényében legalább olyannyira értékes lehet.
- Ne reklámozzuk, hogy milyen eszközök vannak nálunk, ezzel elkerülhetjük, hogy a tolvajok figyelme ezekre terelődjön.
- Utazásaink során amennyiben nincs minden esetben szükségünk ezen eszközökre, ítéljük meg, hogy nem lenne-e érdemes elzárt széfbe helyezni őket. Erre a legtöbb hotel biztosít lehetőséget.
- Adatainkat ne csak ezen eszközökön tároljuk, készítsünk róluk biztonsági másolatot.
- Amennyiben van rá lehetőségünk, titkosítsuk az eszközök adattároló részét.

Természetesen a leginkább elővigyázatos emberekkel is előfordul, hogy ellopják eszközeiket. Amennyiben ez bekövetkezne, azonnal jelentsük a lopás tényét a megfelelő hatóságnál. Abban az esetben, ha az eszköz munkahelyi szenzitív adatokat is tartalmaz, figyelmeztessük az illetékes munkatársunkat, hogy megtehessék a szükséges lépéseket. [11][12]

7. Kiemelten veszélyeztetett személyek

A gyermekek és időskorúak számára is az Internet új távlatokat nyit meg, azonban szem előtt kell tartanunk, hogy ők, személyükből fakadóan különösen veszélyeztetettek. Természetesen a két kategória más és más veszélyeknek van kitéve, és ezeket másképp kell kezelni. Cikkünkben pedig, lévén, hogy az informatikaoktatás leginkább őket érinti, a gyermekekre térünk ki.

Amikor egy gyerek játszik a családi számítógépen, nem feltétlenül gondolunk arra, hogy ez a tevékenység káros lehet, azonban pont abból kifolyólag, hogy az illető nincs tökéletesen tisztában azzal, hogy mit csinál, ez biztonsági kockázatot jelent. A támadók könnyebben tudnak információt kicsikarni belőle, egyszerűbben rá tudják venni olyan weboldalak meglátogatására, melyek rosszindulatú kódokat szeretnének számítógépünkön futtatni, amennyiben pedig ez egy olyan eszköz, melyet a család más tagjai szenzitív adatok tárolására használnak, a probléma már adott. Mit tehetünk, hogy a gyermek biztonságosabban tudja használni a számítógépet és az online teret?

- Váljunk érintetté a gyermek számítógépes tevékenységében. Ajánljuk fel neki, hogy csatlakozunk hozzá, miközben játszik, találjunk ki olyan feladatokat, melyek során jó példával járhatunk elől a biztonságos böngészést illetően.
- A gyermek által is használt számítógépet lehetőleg ne használjuk szenzitív adatok tárolására, azt helyezzük a lakás olyan pontjára, ahol általában rálátunk (például a nappaliba), így ha valami problémát észlelünk, azonnal be tudunk avatkozni.
- Tisztázzuk a gyermekkel, hogy mit tehet meg és mit nem számítógép előtt töltött idejében. Ezen korlátok természetesen az érintett életkorához, tudásához kell hogy illeszkedjenek.
- Monitorozzuk a gyermek számítógépes tevékenységét, állítsunk be szülői felügyeletet, melyre a legtöbb operációs rendszer lehetőséget biztosít.
- Folyamatosan álljunk készen arra, hogy amennyiben a gyermeknek kérdése van, számára érthetően meg tudjuk azt válaszolni, legyen az bár egy tiltással, bár egyéb kéréssel kapcsolatos. Legyen a célunk az, hogy biztonságtudatosságra neveljük gyermekeinket.

- Amennyiben többen használják az adott eszközt, alakítsunk ki külön partíciókat, melyekhez csak azok tulajdonosai férhetnek hozzá. [13]

8. Összegzés

Tanulmányunkban, a mindennapi életben is használatos biztonsági irányelveket prezentáltuk, melyekről az a véleményünk, hogy az információs társadalom életében meghatározó fontosságúak. Úgy véljük, hogy bármely informatikaoktatásban résztvevő tanár elő tudja segíteni tanulói online boldogulását, ha ezen irányelvek mentén figyelmezteti őket az Internet lehetőségei mellett annak veszélyeire is, és megtanítja őket milyen lépéseket tehetnek, hogy csökkentsék az áldozattá válás kockázatát.

Köszönetnyilvánítás

A szerzők köszönetüket fejezik ki az Ericsson Kft. irányába az ELTE CNL együttműködésben nyújtott támogatásukért.

Irodalom

1. *Why is Cyber Security a problem?* (elérés dátuma: 2015.11.03.)
https://www.us-cert.gov/ncas/tips/ST04-001
2. Choosing and protecting passwords (elérés dátuma: 2015.11.03.)
https://www.us-cert.gov/ncas/tips/ST04-002
3. Guidelines for publishing information online (elérés dátuma: 2015.11.03.)
https://www.us-cert.gov/ncas/tips/ST05-013
4. What is my IP address? (elérés dátuma: 2015.11.03.)
http://whatismyipaddress.com/
5. How anonymous are you? (elérés dátuma: 2015.11.03.)
https://www.us-cert.gov/ncas/tips/ST05-008
6. Understanding web site certificates (elérés dátuma: 2015.11.03.)
https://www.us-cert.gov/ncas/tips/ST05-010
7. Browsing safely: Understanding Active content and Cookies (elérés dátuma: 2015.11.03.)
https://www.us-cert.gov/ncas/tips/ST04-012
8. Social Networks – Statistics and Facts (elérés dátuma: 2015.11.03.)
http://www.statista.com/topics/1164/social-networks/
9. M. McDowell, and D. Morda: *"Socializing securely: using social networking services."* United States Computer Emergency Readiness Team (US-CERT), Washington, DC (2011).
10. Staying safe on social networking sites (elérés dátuma: 2015.11.03.)
https://www.us-cert.gov/ncas/tips/ST06-003
11. Protecting portable devices: Physical security (elérés dátuma: 2015.11.03.)
https://www.us-cert.gov/ncas/tips/ST04-017
12. Protecting portable devices: Data security (elérés dátuma: 2015.11.03.)
https://www.us-cert.gov/ncas/tips/ST04-020
13. Keeping children safe online (elérés dátuma: 2015.11.03.)
https://www.us-cert.gov/ncas/tips/ST05-002