Szent István Egyetem
Gazdaság- és Társadalomtudományi Kar
Tudományos Diákköri Konferencia
Gödöllő, 2016. november 23.

Az információs biztonságvédelem tudatosságának vizsgálata a ma élő hat generáció hozzáállásának tükrében

Evaluation of information security and protection awareness of the living six generation

Készítette: Ganczer Laura, SZIE GTK Bsc EE III. évf.
Nappali tagozat, Budapesti Képzési Hely

Konzulens: Dr. Szilágyi Tivadar, tanszékvezető egyetemi tanár, SZIE GTK RGVI, Civil Biztonság- és Védelemtudományi Tanszék

OTDK szekció: Had- és Rendészettudományi

Gödöllő, 2016.

Tartalom

1. BEVEZETÉS

A Szent István Egyetem végzős hallgatója vagyok, Emberi erőforrások szakon. Az egyetemen eltöltött eddigi két év során, olyan szabadon választható tantárgyak mellett döntöttem, amelyek egymásra épülnek; a biztonság és a védelem kultúrája, civilbiztonság és a vidékbiztonság. E tantárgyak hallgatása közben, valamint az év végi beadandó dolgozat megírásának köszönhetően egyre érdeklődőbbé váltam a tantárgy keretein belül tanultakkal kapcsolatban, különösen az információs biztonság témakörében merültem el. Az egyik dolgozatom az informatikai biztonság témakörében íródott, ezt követően kezdtem el behatóbban foglalkozni ezzel a területtel, és igyekeztem kiszélesíteni a látóköröm ezzel a témával kapcsolatban. Felkeltette az érdeklődésem az információs és az informatikai biztonság közötti különbség mibenléte, továbbá kíváncsiság merült fel bennem, azzal kapcsolatban, hogy vajon lehet-e párhuzamot vonni, a manapság népszerű generációs jellemzések és az információs biztonság tudatosságával kapcsolatban?

Dolgozatomban az információs biztonság komplex értelmezésére vonatkozó szakirodalmat fogom áttanulmányozni és bemutatni a fogalmakat, különbséget tenni az információs és az informatikai biztonság között. Emellett bemutatom a ma élő hat generáció besorolására vonatkozó szempontokat és az egyes generációk jellemzőit. A virtuális világban, az online felületen és a hétköznapi élet során felmerülő veszélyek ismertetése lényeges része a dolgozatomnak, s az erre vonatkozó kérdések feltevése jelen lesz a kérdőíves kutatásomban, amely segítségével kívánom megállapítani, hogy mennyire tudatos a ma élő hat generáció az információs biztonság területén. Továbbá dolgozatomban kitérek a védelmi intézkedések ismertetésére is, be fogom mutatni az Európai Uniós kiberbiztonsági stratégiáját, valamint kifejtem az abban foglaltakat.

A kérdőíves kutatás elemzését követően ismertetem az eredményeket és abból következtetéseket vonok le, azzal kapcsolatban, hogy melyik generáció milyen szintű figyelmet fordít az említett információs biztonsággal kapcsolatos kérdésekre, valamint mértékadó javaslatokat fogok tenni arra vonatkozóan, hogy milyen irányban lenne érdemes továbbvinni ennek a témának a vizsgálatát, illetve kezelését a jövőben.

2. AZ INFORMÁCIÓBIZTONSÁG KOMPLEX ÉRTELMEZÉSE

Mostanában az információs társadalomnak köszönhetően számottevő mértékben megnövekedett az információ értéke, jelentősége. Minden eddiginél fontosabbá vált az információhoz való hozzájutás, annak tárolása, és hatékony felhasználása. Ezzel egyidejűleg, pedig törvényszerűen megjelentek az olyan típusú tényked̈ések, amelyek az információhoz való hozzáférés és felhasználás akadályozására, esetleg tönkretételére irányulnak. Az információs társadalomra az információ elsőszámú értékké válása a jellemző. Ezzel együtt jár a számítástechnika és a távközlés rohamos fejlődése, a személyi számítógépek elterjedtek, s megjelentek a gyors adatátviteli hálózatok. Nagy technológiai újítás az internet és a mobiltelefon. Az internet térhódításának köszönhetően új kommunikációs eszközök jelentek meg, amelyek lehetővé teszik a gyors és olcsó kommunikációt az akár nagyobb távolságban lévő emberek között is, viszont a személyes kommunikáció ennek hatására háttérbe szorul.

Ma már az élet egyetlen területén sem nélkülözhető az információs eszközök használata. Ennek megfelelően az információs munkakörökben dolgozók aránya nagymértékben nő, lehetővé válik a távmunka, és szükségessé vált az egész életen át tartó tanulás. Viszont az információs társadalomban élő embernek számos, régebben ismeretlen problémát kell megoldania. Például a terjedelmes, de változó minőségű információ megfelelő értékelése, kiválogatása és feldolgozása, vagy a magánszféra védelme. Ezért napjainkban egyre tudatosabbá válik az igény az információ megóvására, eredményes védelmére. Lényeges kiemelnem a következőt: **az információbiztonság nem egyenlő az informatikai biztonsággal!**

Az információs társadalom működésének alapja az infokommunikációs rendszereken alapuló információs infrastruktúrák egymásba kapcsolódó komplex rendszere; a távközlési, informatikai rendszerek, a hozzájuk kapcsolódó elektronikai rendszerekkel egységes rendszert képeznek, ami által képesek teljes produktivitással működni. Tehát az infokommunikációs rendszerek jóval többet jelentenek, mint kizárólagosan az informatikai és távközlési rendszerek konvergenciájából kialakuló rendszerek. Hiszen ebbe, beletartoznak mindazon rendszerek is, melyek az érzékelés, irányítás, vezérlés funkcióit látják el. Például ebbe a kategóriába sorolhatók azok a repülőtéri leszállító és irányító rendszerek is, amelyek a távközlési rendszereken és a számítógép-hálózatokon keresztül csatlakoznak más rendszerekhez. Rendkívül fejlett információtechnológián alapuló infokommunikációs rendszerekkel látják el a különböző kormányzati, gazdálkodó, védelmi szervezeteket és a vállalatokat. Abban az esetben, ha a szervek ezeket az információs rendszereket megfelelően tudják működtetni,

egyúttal a biztonságos működtetésüket is képesek megteremteni, akkor ez egy erősokszorozó, képesség javító és integráló hatású tényezővé válik.

Az információs társadalom, függő viszonyban áll a funkcionális információs infrastruktúrákkal, például távközlő- és számítógép hálózatokkal, amelyek tevékenysége viszont nem lehetséges a támogató infrastruktúrák; villamos energiaellátó rendszerek effektív működése nélkül. Amennyiben az infrastruktúrarendszer bármely csoportját támadás éri, az közvetlenül vagy közvetve negatívan befolyásolja a másik működését is. A biztonságot fenyegető veszélyek nemcsak a funkcionális infrastruktúrákon keresztül jelentkeznek, hanem az azt támogató infrastruktúrákon keresztül is.

Így leszögezhető, hogy az infrastruktúrák között kölcsönös függőség áll fenn. A támogató információs infrastruktúrákon keresztül az információs társadalom funkcionális információs infrastruktúráinak működését károsan lehet befolyásolni: zavarni, korlátozni, megszüntetni.

Például az ipari kémkedés esetében, amikor olyan kutatás-fejlesztési és gyártási adatokhoz, információkhoz jutnak, amelyet felhasználva hamarabb tudnak különböző termékeket piacra dobni, és ez által jelentős előnyre és profitra szert tenni a versenytársakkal szemben. A fenyegetések indíttató tényezői különböző politikai, gazdasági, pénzügyi, katonai, szociális vagy egyéni célok elérése lehet. Az infokommunikációs rendszerek elleni fenyegetések formái és szintjei, a konfliktus helyzetek, a technikai lehetőségek, és a motivációk szerint változhatnak. Jelentőségüket tekintve ezek a veszélyforrások, illetve az általuk adott esetben okozott károk több rendszerben együttesen jelentkeznek. Egy „jól megválasztott” támadás, amely egy infokommunikációs rendszer ellen irányul, akár egy egész ország, vagy akár egy szub-regionális infokommunikációs rendszer sérüléséhez, vagy akár teljes leálláshoz vezethet. Az információs társadalom infokommunikációs rendszerei elleni fenyegetések a következők lehetnek:

- illetéktelen hozzáférés az információkhoz
- rosszindulatú szoftverek bevitele a rendszerbe, ezáltal ellehetetleníteni annak működését
- rosszindulatú szoftverek útján az adatbázis lerontása, módosítása, felhasználhatatlanná tétele
- az infokommunikációs rendszer adatainak megszerzése
- elektronikai támadások; zavarokkal vagy megtévesztésekkel egyaránt támadhatók a katonai és a polgári kommunikációs rendszerek

A fenyegetések származhatnak személyektől, terroristáktól, különböző nemzeti szervezetektől,

külföldi hírszerző szolgálatoktól vagy akár katonai szervezetektől is. Az infokommunikációs rendszer elleni tevékenység eredetét nehéz azonosítani, ráadásul e csoportok között a határok elmosódnak.

A komplex információs támadás, és ebből adódóan az összetett védelem is, céljai elérésének érdekében fizikai-, információs- és tudati kiterjedéseiben fejti ki hatásait.

A fizikai dimenzióban folytatott információs tevékenységek a különböző információs infrastruktúrák, infokommunikációs rendszerek elemei elleni támadását, és az azokkal szembeni fizikai védelmet jelentik.

Az információs dimenzióban folytatott információs tevékenységek a különböző információs folyamatok, adatszerzés, adatfeldolgozás, kommunikáció, stb. többnyire elektronikus úton való támadását jelenti, fizikai ráhatás nélkül közvetlenül befolyásolják azokat. Másik oldalról ide tartozik a másik fél saját információs folyamatainkra irányuló hasonló támadásának megakadályozása.

A tudati dimenzióban megvalósuló információs tevékenységek közvetlenül az emberi gondolkodást — észlelést, érzékelést, értelmezést, véleményt, vélekedést — veszik célba valós vagy hamis üzenetekkel, amelyeket többnyire elektronikus és nyomtatott médián keresztül vagy közvetlen beszéd formájában továbbítanak.

A digitális szakadék fogalma a modern információs és kommunikációs eszközök, mint például a telefon, a számítógép, az internet, használati szokásaihoz kapcsolódik, különbségek a hozzáférésben és kezelési alapismeretekben van. Egyes emberek szinte a mobiltelefonjukkal összenőve élnek, míg mások egyáltalán nem is tudnak kezelni ilyen készülékeket, nem alkalmazzák a modern eszközöket.

Két adat az Eduline 2009-es cikke alapján:

- A 13-16 évesek felének van internet-kapcsolata, átlagosan 2, 2 órát töltenek a gép előtt. Majdnem mindegyiküknek van saját mobiltelefonja.
- Háromból egy tinédzser képtelen lenne a számítógépe nélkül élni, ötből egy pedig a tévé nélkül.

A „digitális vízválasztók” egyre nőnek a családokban. Míg a gyermek szinte percek alatt mesterévé válik az internetnek és a videojátékoknak, addig a szülőknek és a nagyszülőknek fogalmuk sincs, mit látnak. Az idősebb generációnak nagyon nehezére esik felfogni és megérteni, mi is történik a gyerek szobájában, mivel ők teljesen más módon kommunikálnak.

A kutatásom célja az is, hogy kiderítsem, a generációk között milyen mértékű digitális szakadék van jelen napjainkban. Hiszen egy Veterán generáció szülötte ember lehetséges, hogy tisztában sincs olyan fogalmakkal, amelyek a fiatal generációk számára a minden napi csevegés alap szókészlet alkotórészei. Annak érdekében, hogy behatóbban megismerjük a generációk jellemzőit, illetve a köztük fellelhető különbségeket, dolgozatom következő fejezete erről fog szólni. [1] [2] [3]

3. GENERÁCIÓK BEMUTATÁSA

Ebben a fejezetben bemutatom a ma élő hat generáció tulajdonságait. A generációkat a születési évük alapján soroljuk be az alábbi táblázat szerint, ez összefoglalja a generációk elnevezését.

1. táblázat: Generációk jellemzői [4]

A GENERÁCIÓ ELNEVEZÉSE	SZÜLETÉSI IDŐ	AZ ELNEVEZÉS EREDETE
Veterán (csendes) generáció	1925-1945	A világháborúkat megélt generáció
Baby boom generáció	1946-1964	A II. világháború utáni népességrobbanás gyermekei
X generáció	1965-1979	(Coupland, 2007) generációs műve után
Y generáció	1980-1994	Az X generáció után következő
Z generáció	1995-	Az Y után következő
Alpha vagy Új csendes generáció	2010-	A Z után következő α (alfa) generáció

3.1. A Veterán generáció

Jellemzően egy munkaadónál, egy szakterületen dolgoztak egy életen át, már jellemzően nem aktív munkaerő-piaci generáció. Egy új világot építettek fel, ahol értékes tudást és tapasztalatot halmoztak fel. A generáció a 20. század nehéz éveiben nőtt fel és szocializálódott; megtanulták, hogyan kell túlélni a háborúban, a fronton és a rendszerek változásában, s mint a háború és a világválság gyermekei olyan környezetben nőttek fel, amelyben az alkalmazkodás a siker záloga. Számukra érték egy munkahelyen ledolgozni az életüket és kiemelten fontos a hiteles, céltudatos, karizmatikus vezető személye. Tisztelik a kétkezi, fizikai munkát és az életkorhoz köthető tapasztalatnak nagy tekintélye van köreikben.

3.2. A Baby-boom generáció

A szüleiktől az különbözteti meg őket, hogy új utakra, tudásra, információra, cselekvésre vágynak, karriert építenek. A demográfiai robbanás gyermekei. Alázattal végzik munkájukat, fegyelem, tisztelet és kitartás jellemzi őket. Kötődnek a munkahelyhez, az íróasztalukhoz, fontosak számunkra a státuszszimbólumok, amely a hierarchiában betöltött szerepekhez köthetők. Tudásuk, tapasztalatuk, bölcsességük, munkafegyelmük és lojalitásuk olyan érték, amely bármilyen és bármekkora céget a legjobbak közé emelhet. Tartanak attól, hogy az utánuk következő nemzedékek elveszik a munkájukat, mert olyan készségekkel rendelkeznek, amikkel ők nem.

3.3. Az X generáció

Elődeiknél magasabban iskolázottak, sokuknak két vagy több diplomája is van. Az X generáció tagjai már két-jövedelmű családokba születtek, ahol a válás is megszokott jelenség volt. A nők tömegesen csatlakoztak a munkaerő-piaci folyamatokba, sok gyerek nem is látta a szüleit, mert azok mindketten dolgoztak. Így a "kulcsos gyerekek" generációja önálló, találékony és önellátó nemzedékké vált, akik a munkahelyen is értékelik a szabadságot és a felelősséget. Az első generáció, akik már kamaszként is találkoztak számítógépekkel, a technológiai fejlesztések begyűrűztek életükbe, ők pedig - lassan vagy gyorsabban - meg tanulták kezelni azokat. Munkába állásukkor a munkaerőpiacon versenyképes fizetést kínáló, újonnan betelepült multinacionális vállalatok várták őket, akikkel együtt azonban megérkezett a korlátlan munkaidő és a korátlan munkahelyi stressz is.

3.4. Az Y generáció

Nyitottak az újdonságokra, befogadóak, gyorsan sajátítják el a technológiai újdonságokat. Internetes személyiséggel és új kommunikációs stílussal rendelkeznek. A számítógépekkel együtt nőttek fel, igen gyakorlatiasak, és remekül eligazodtak az interneten. Nem tudnak mindent fejből, de tudják, hogy keressék a szükséges információt. Társadalmi kapcsolataikat egy időben élik meg a valós és a virtuális világban. Új világot építenek, hiszen nem a hagyományos irodai munkakultúrát képviselik, hanem a mobil és az internet segítségével a világ bármelyik pontján elvégzik feladataikat, létrehozva virtuális közösségeiket. Elődeiket megszégyenítő önbizalommal szállnak szembe a megkövült szabályokkal, más képességekkel rendelkeznek, mint az előző generációk. Az Y generáció élvezni akarja a munkahelyet: legyen az modern, ugyanakkor kiemelten fontos számunókra a munka és a magánélet egyensúlya. Ők a fordított szocializációs generáció, ami annyit jelent, hogy a legfontosabb tudást, amely a

digitális újkorban szükséges nem az előző generációktól szerzi meg, hanem saját maga által és kortársaitól. Sőt, ő tanítja az előző generációkat a digitális világ eszközeinek használatára.

3.5. A Z generáció

Ők már teljes egészében beleszülettek abba a világba, amelyet egyre inkább meghatároznak a különböző digitális technológiák. Z - más források szerint R-nek (responsible) nevezett - generáció, a világ első globális nemzedéke, akik ugyanazon a zenén, ételen, és divatirányzaton nőnek föl, a legkisebb létszámú, a legoktatottabb, a legkisebb családba született, a legidősebb anyák nevelik (és sokszor egyedül) és az előző generációkhoz képest hosszabb várható élettartammal rendelkeznek. Hozzászoktak ahhoz, hogy állandó kapcsolatban vannak egymással, hogy állandó, korlátlan és azonnali hozzáférésük van a világhálóhoz. Hálózaton keresztül funkcionálnak a legjobban, a szocializáció ebben a korosztályban virtuális térben történik. Profin kezelik az elektronikus eszközöket, a közösségi oldalakon ezernél több baráttal rendelkezhetnek, a való életben zajló kommunikációt, azonban stresszhelyzetként élik meg, ezért egyre inkább bezárkóznak, a valódi világban leépítik baráti körüket és az internet nyújtotta biztonságba menekülnek.
Információforrásuk leginkább a web. Jellemző rájuk a párhuzamos cselekvés.A Z generáció ösztönösen olyan képességekre, készségekre tesz szert, mint a többfeladatos működés/feldolgozás (multitasking), az együttműködő tanulás (hálózatban, collaborative) vagy az önszabályzó tanulás. Ez a generáció mindezekre a készségekre az iskolán kívül, szabadidejében tesz szert, kizárólag önszabályozó módon, illetve hálózatban korcsoportjától tanulva.

3.6. Az Alpha generáció

Ez a generáció a második Baby boom generáció, ahogyan az elsőnek, úgy nekik is komoly technológiai és társadalmi változásokkal kell majd szembesülniük.
A legtovább fognak élni az emberiség történetében, a legmagasabb iskolai képzettséggel rendelkeznek majd és teljes mértékben a világháló részei lesznek. Ennek az ára, hogy ők lesznek a legmagányosabb nemzedék, akik a GOOGLE szemüvegeken keresztül folyamatos hálózati kapcsolatban állnak majd egymással, de egykék lesznek és egyedül fognak élni is.
A generáció olyan problémákra kell, hogy megoldást találjon, mint a környezetszennyezés, globalizációs ártalmak és a társadalmi öregedés. Ezért is nevezik őket "új csendes, vagy alfa" generációnak, remélve azt, hogy képesek lesznek a kihívásokkal megbirkózni, és azt, hogy velük újra kezdődik minden, új lehetőséget kapnak, amivel élni is tudnak majd. [5]

Ahogy a biztonságtechnika egészére igaz, úgy az információbiztonság részterületére is, hogy a legnagyobb veszélyt az emberi tényező jelenti. Míg a technikai eszközök megbízhatósága egzakt módon mérhető, addig a humán erőforrás számottevő bizonytalansági faktorként van jelen a rendszerekben. Dolgozatom célja, hogy megismerjem a különböző generációk hozzáállását a technikai eszközök, közösségi oldalak biztonságos használatával tisztában vannak-e, továbbá, hogy milyen tudatossággal állnak ezekhez a kérdésekhez. A következő fejezetben ismertetni szándékozom az általam veszélyesnek tartott területeket az információs biztonság témakörein belül.

4. A VIRTUÁLIS VILÁG FELHASZNÁLÓIRA LESELKEDŐ VESZÉLYEK

4.1. Gyerekekre, tinédzserekre leselkedő veszélyek a világhálón

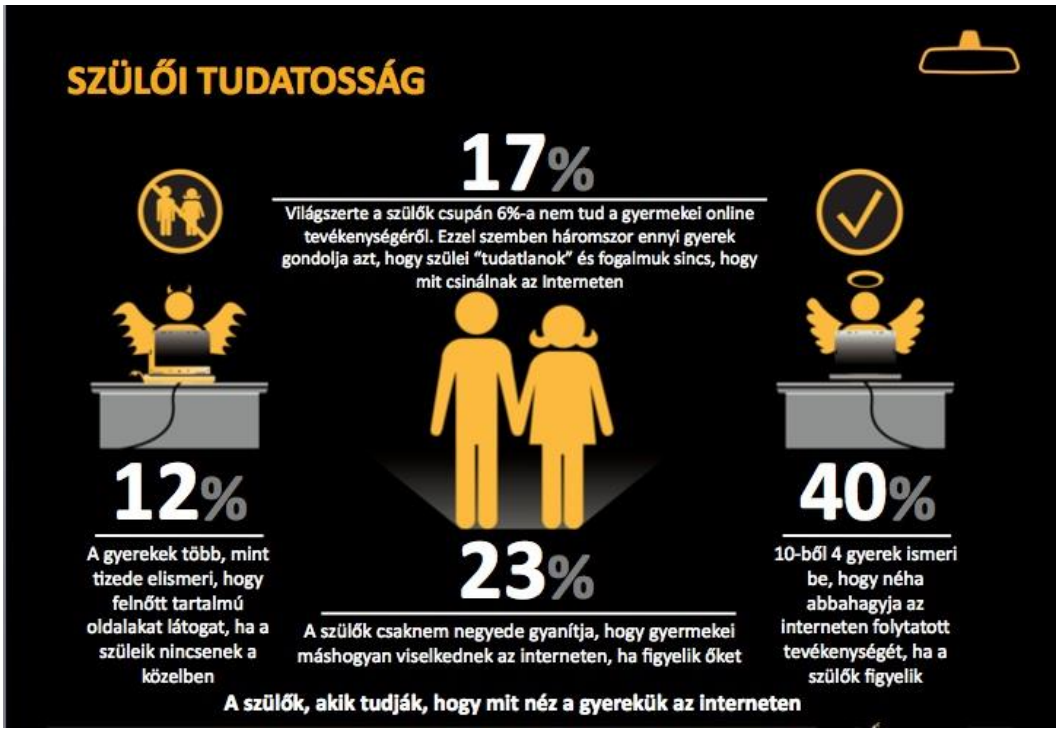
A gyerekek rengeteg időt töltenek az internet virtuális világában. A közösségi oldalakon sokszor túl sok személyes adatot és információt szolgáltatnak magukról. Számos esetben a közösségi oldalon töltik éjjelüket-nappalukat a mai kamaszok. Ezek a portálok remek lehetőséget jelentenek számukra a másokkal való megismerkedésre, és a barátokkal való kapcsolattartásra, a kommunikáció egy teljesen új dimenziója nyílik meg előttük. Azon felül, hogy a gyerekek személyes adatotokat adhatnak meg magukról, olyan témákról is beszélgethetnek idegenekkel, amely témák nem nekik valóak.

Miért vonzóak ezek az oldalak? Arctalanul, fiatalkori gátlásaikat levetkőzve tudnak kommunikálni osztálytársaikkal, barátaikkal, a felöltött tartalmakkal kedvelést érhetnek el a társaik körében. Más részről, például online játékok segítségével megismerkedhetnek új emberekkel, akikkel közös az érdeklődési körük, és adott esetben egy „chat” kapcsolat indulhat el közöttük. Szintén lényeges faktor, hogy egy idegennek, arctalanul könnyebben ki tudják önteni a szívüket, mesélnek a személyes problémáikról, amikről esetleg nem mernek a szüleiknek, testvéreiknek, osztálytársaiknak beszámolni. Ez a folyamat végzetes eseményekbe is torkollhat. Hiszen, ha egy pedofil hamis internetes személyiséggel teremt bizalmi kapcsolatot az ártatlan gyermekkel, fiatallal egy megbeszélt személyes találkozás során el is rabolhatja a gyereket. Belegondolni is borzalmas az ilyen következményekbe, így minden szülőnek résen kell lennie gyermeke lelkiállapotával, baráti kapcsolataival és főleg, oda kell figyelniük arra, hogy milyen gyakran használ számítógépet a fiatal és, hogy milyen oldalakat látogat rendszeresen. Napjainkban a legtöbb zenei videoklip sokszor tarthatatlan képekkel, jelenetekkel van tele. Amennyiben a gyerek már nagyobb, és egyedül használja a számítógépet, akkor van olyan lehetőség, hogy beállítjuk a „szülői felügyelet” funkciót, amellyel megadhatjuk például,

hogy mely órákban használhatják a számítógépet, melyik játékokkal játszhat, és milyen programokat futtathat, milyen honlapokat tiltunk le a számára. Ha a szülői felügyelet blokkol egy játékot vagy programot, akkor ezt egy értesítésben jelzi. Gyermekünk az értesítésben található hivatkozásra kattintva engedélyt kérhet, hogy hozzáférhessen az adott játékhoz vagy programhoz. Az elérést fiókinformációink megadásával engedélyezhetjük.

Véleményem ez egy rendkívül hasznos lehetőség, de nem nyújt teljes biztonságot. Sokszor látom azt, hogy a szülők nem elég tudatosan kezelik ezt a problémát, vagy nem is gondolnak erre, mint probléma lehetőségre. Hiszen már egyre kisebb korban profin nyomkodják a kis ujjacskák az okos telefonokat, tableteket, miközben az édesanya hajat szárít nekik az uszodában, sorban állnak a boltban, sorolhatnánk. Először 2013-ban, majd 2014-ben merült fel az a rémhír, hogy a „Talking Angela" (beszélő Angela) című okos telefonalkalmazást pedofilok használják áldozataik becserkészésére. Egy internetes beszámoló szerint az alkalmazás kihúzza a gyerekek nevét, lakcímüket, titokban fotót készít róluk és arra is rákérdez, hogy kivel vannak, merre mennek haza az iskolából. Állítólag, a Naked Security, ami egy információs technológia biztonsági blog megcáfolta ezt a tévhitet. Mindenestre elgondolkodtató, hogy mennyi az esély a hasonló jellegű történésekre a jövőben. Időnként lehet hallani, főleg külföldről jönnek a hírek, hogy tinédzsereket az interneten keresztül beszerveznek különböző vallási szektákba, újabban szaporodik azok száma, akikről kiderült, hogy az ISIS terrorszervezet tagjai interneten keresztül szervezték be, utaztatták őket és velük, európai állampolgárokkal végeztetett el bűncselekményeket, terroristatámadásokat.

Meglátásom, hogy a gyerekekre nagyon kell vigyáznunk és több szempontból is aggályos a generációk hozzáállása a rájuk irányuló információs biztonság kérdésével kapcsolatban. Hiszen a Veterán, a Baby boom és az X generáció nem ismeri még az internetet és a benne rejlő veszélyeket, amikor az Y generációs, Z generációs gyermekük, unokájuk ismerkedik vele. Így felkészületlenek a pedofilok trükkjeire, a chat szobákban zajló ismerkedésre, ahol mindenki annak adja ki magát, akinek akarja. Sajnos, számos borzalmas eset történt, amikor elcsaltak kisgyerekeket, miután az interneten megismerkedett velük és a bizalmukba férkőzött az elrablójuk. Az Y generáció, mint szülő minden bizonnyal tudatosabban odafigyel már ezekre a veszélyekre és képes alkalmazni a „szülői felügyelet" funkciót, ugyanakkor elképzelhető, hogy számára már olyan evidens az internet használata, hogy nem foglalkozik olyan mértékben a lehetséges veszélyekkel szembeni védelemmel, mint amilyen mértékben szükséges lenne.



1. ábra: Szülői tudatosság [6]

A Norton Online Family 2011-es jelentése örömre adhat okot, hiszen világszerte mindössze 6%-a a megkérdezett szülőknek felelte azt a felmérésen, hogy nincs tisztában a gyermeke online tevékenységével. A gyermekek háromszorosa vélekedek sajnálatos módon ennek az ellenkezőjéről. Tehát a szülőknek érdemes lenne a jelenleginél is jobban követni gyermekeik online tevékenységét, hiszen a válaszoló gyermeket 12%-a elismerte a felmérés során, hogy felnőtt tartalmú oldalakat látogat meg a szülei jelenlétének hiányában.

4.2. Közösségi oldalak, a Facebook veszélyei a felhasználók vonatkozásában

Amikor valamilyen információt osztunk meg a Facebookon, adatlapunkra, illetve mások adatlapjára feltöltve, ezek az információk a feltöltést követően azonnal kikerülnek az ellenőrzésünk alól. Így még szigorú adatvédelem alkalmazása is könnyen nyilvánossá válhat a feltöltött tartalom. A Facebookon a legszigorúbb adatvédelem, amikor csak saját magunk olvashatjuk posztjainkat, de ezt megtehetjük offline is, ehhez nem kell hozzá feltölteni semmit. Abban az esetben, ha sok online barátunk van, egyáltalán nem lehetünk biztosak abban, hogy mindegyikük ugyanolyan gonddal megőrzi a ránk vonatkozó információkat, mint mi magunk, így visszaélés áldozataivá válhatunk, ráadásul az ismerőseink ismerősei is számos esetben meg tudják nézni a képeinket, azokat is, amelyeket mi magunk töltöttünk fel, illetve amin mások jelöltek be minket. Itt szeretném megemlíteni, hogy lehetséges annak a beállítása, hogy a jóváhagyásunk nélkül senki se jelölhessen be minket képen. A fiatalabb generáció, a Z

generáció gyermekeire jellemző manapság, hogy ismerősöket gyűjtenek, valódi ismeretség nélkül is, hiszen az a menő, akinek minél több ismerőse van. A cél a bűvös ötezres szám elérése, ennyiben maximálja mostanság a Facebook a barátok számát. Így rengeteg idegen ember kerül bele abba a körbe, amellyel megosztjuk a feltöltött tartalmakat, tehát hatványozódik a megbízhatatlan emberek száma, akik tudomást szereznek adatainkról. Ráadásul olyan emberek is bekerülhetnek virtuális ismeretségi körünkbe, akik hamis adatokkal, hamis profillal, másoktól ellopott képekkel vannak fent az oldalon, valószínűleg ha már ilyen csaláson alapuló regisztráltak, nem pozitív indíttatásból tették ezt meg, tehát veszélyt jelenthetnek ránk. Érdemes tehát odafigyelni arra, hogy kizárólag olyan személyeket jelöljünk vissza a közösségi oldalakon, például a Facebookon, akiket valóban ismerünk. Továbbá, hogy megfontoltan töltsük fel a rólunk szóló információkat, a nagyvilág számára, de a lehető legjobb, ha nem töltünk fel ilyet, hanem arra használjuk az oldalt, amire való; kapcsolattartásra.

4.3. Hölgyekre leselkedő veszélyek a világhálón

Saját tapasztalat a következő; rendkívül ijesztő volt azzal szembesülnöm, hogy az elmúlt hónap során többször jelöltek ismerősnek közösségi oldalon, igen gyanúsnak tűnő figurák. Megnéztem az adatlapjukat, hogy hol laknak, mivel foglalkoznak, hány ismerősük van, és milyen benyomást kapok az illetőről ezek alapján. Természetesen egy percig sem fontolgattam az ismerősnek jelölés elfogadását. Ugyanakkor tájékozódásképp, a mai világ új keletű veszélyeivel tisztában vagyok, így megnéztem az adatlapjaikat. Sajnálatos módon azt láttam, amire számítottam. Gyanús alakoknak tűntek a pár darab fotó alapján, amiket feltöltöttek, és az ismerőseikről az szűrhető le, hogy zömmel gyanús külsejű férfiak, illetve feltűnően fiatal lányok. Kevés ismerőssel rendelkeztek, bevándorlóknak tűntek, nagycímletű pénzekkel fényképeztették le magukat, sorolhatnám. Szerencsére konkrét erőszakos cselekmény ábrázolása nem volt a képeken, de véleményem szerint elgondolkodtató, hogy a mostanában történt magas számú bevándorlást, migrációt követően fiatal huszonéves, gyanús külsejű férfiak európai lányokat jelölgetnek randomra a közösségi oldalakon. Feltételezem, hogy ezzel a dologgal előbb utóbb a házasság lehet a hosszú távú céljuk, már amennyiben valakivel létrejön. Hiszen akkor megkapják az európai állampolgárságot, amivel aztán szabadon mozoghatnak az Európai Unió területén.

Már évekkel ezelőtt felütötte a fejét az a probléma, hogy európai nők külföldön töltött nyaralásuk során hagyták elcsavarni a fejüket és szerelembe estek arab, török férfiakkal, akikről később kiderült, hogy csalók, pénzre, állampolgárságra utaztak, és gyakran már családdal rendelkeztek, úgy vették el második feleségként az átvert európai hölgyeket. Létezik egy lista,

a „Bezness Alert”, amely egy angol nyelvű honlap, ahol erre a jelenségre figyelmeztetik a nőket, megnevezve a csalókat, korábbi megtörtént történeteket elmesélve.

4.4. Internet segítségével történő térítés, toborzás

Napjainkat egyre inkább áthatják a terrorszervezetek által elkövetett támadások borzalmas hírei. Egyre általánosabbá váló jelenség, hogy abban az országban született, szocializálódott és élte mindennapjait a szörnyű gyilkosságok merénylője, mint ahol ezeket elkövette.

Körülbelül 2009-ben készítettek egy toborzást segítő kézikönyvet, amely útmutatásként szolgál a terrorszervezetek tagjai, szimpatizánsai számára, hogy miként szerezzenek, illetve szervezzenek be jelenleg kívülállókat, céljaik elérésének érdekében. Előnyt élveznek azok az emberek, akik nem gyakorolnak vallást, nem vallásosak, mivel egyszerűbb így a térítésük. A vallástalanok mellett megfelelő célpontnak számítanak a vidéki főiskolás, egyetemi hallgatók, hiszen tele vannak tettvággyal. Az első feladat a célpont megkörnyékezése, ezután megkezdődik a vallási meggyőzés. Ehhez készültek kézikönyvek, amelyek keresztények és zsidók számára is bebizonyítják, hogy az iszlám miképpen javítja ki a korábbi vallások hibáit. Ezt olyan Ó- és Újszövetségi idézetekkel támasztják alá, amelyek alapjaiban megrengethetik az elbizonytalanított célpont addigi hitét. Kezdetben ezek a térítők nem említik valódi szándékukat, hanem kedvesen, figyelmesen ismerkednek. Meghallgatják a jelölt személyes problémáit, és magas fokú egyetértésről, támogatásról adnak hangot. Ezután, miután már kialakult valamelyest a bizalom, a térítők megmutatják, hogy hazájukban milyen borzalmakat követnek el ellenük. Hamarosan megjelenik a szimpátia érzete az áldozatban. Majd a következő fázis során, miután kialakult ez a szimpátia, finoman rávezetik a kinézett személyt arra, hogy kezdje el az elhatárolódást a nem-muszlimoktól. Az utolsó szint, amikor már a markukban van az áldozat, megkezdődik a radikalizálódás, amiknek végeredményeképpen terrorcselekmények elkövetésére, illetve közbenjárására veszik rá az illetőt. A következő webcímen érhető el a pszichológiailag rendkívül hatásos térítői kézikönyv, ellenőrző kérdésekkel, alapos lépésekre lebontott cselekvési tervvel. [7] Megdöbbentő, hogy 10 évvel ezelőtt ez a jelenség elképzelésem szerint elképzelhetetlen volt az online tér világában, mára azonban ezektől a veszélyektől is óvnunk kell a fiatalabb, felnövekvő generáció gyermekeit.

4.5. A kiberbűnözés és a hackerek

A 2000-es évek elején hatalmas változás következett be a kibertéren elkövetett bűnözés területein, korábban a kiberbűnözés unatkozó diákok szabadidős tevékenysége volt, erre az időszakra viszont jellemzővé vált a hackerek csoportokba tömörülése, amely hatására csoportos támadásokat kezdtek el indítani például bankok felületei ellen, pénzszerzés céljából. Eugene Kaspersky, egy orosz zámítógépes biztonsági megoldásokat kínáló cég alapítója nyilatkozatából idézek: *"Az elmúlt években többször láttuk, ahogy a hackerek például benzinkutak rendszerét támadták meg, hogy üzemanyagot lopjanak, vagy szénbányák számítógépes hálózatába hatoltak be. Sőt, tengeri kikötők rendszerét feltörve észrevétlenül csempésztek drogot".*

Az idézett cikk [8] írója szerint a hackertámadások 90%-a banki rendszerek ellen történik. De kik is azok a hackerek és mit csinálnak? A fogalmat tisztázom és bemutatom tevékenységeiket a következő alfejezetben.

4.5.1. A hacker fogalom jelentése, tevékenységük vázolása

A „hacker" szónak a következő a hagyományos jelentése: A hacker kifejezés alatt olyan számítástechnikai szakembert értünk, aki bizonyos informatikai rendszerek működését a publikus vagy a mindenki számára elérhető szint fölött ismeri. Ezek a szakemberek a számítástechnika egy vagy több ágát rendkívül magas szinten művelik, nagyon gyakran ők azok, akik „létrehozzák" azokat az eljárásokat, amik alapján a számítógépek vagy a hálózatok működnek. A jelenkori terminológiában a „hacker" szót hol a „klasszikus hackerekre", hol a „crackerekre", leggyakrabban pedig a komoly szaktudás nélküli internetes vandálokra és bűnözőkre is használják, általában a szakemberek tiltakozását figyelmen kívül hagyva, és így a szó jelentése fokozatosan eltolódik a média által használt értelmezés felé. Tavaly augusztusban egy amerikai hírügynökség rendszerét törték fel, ahonnan több mint 100 ezer vállalati közleményt tulajdonítottak el, később ezeket az információkat eladták. Idén is számtalan hackertámadás történt, amelyekből szeretnék ismertetni párat a továbbiakban. Júniusban Észak-koreai hackerek dél-koreai vállalatbirodalmak és kormányzati hivatalok több mint 140 ezer számítógépét törték fel, majd rosszindulatú kódokat telepítettek rájuk, hogy egy nagyszabású kibertámadást hajtsanak végre, amelyet azonban sikerült meghiúsítani. Szintén 2016 júniusában történt, hogy Donald Trumpról, amerikai elnökjelöltről gyűjtött anyagokat loptak el a hackerek, akikről nyomozók megállapították, hogy vélhetően az orosz kormányzat megbízásában dolgoztak. A www.hvg.hu júniusi cikke [9] figyelmezteti arra a céges dolgozókat, hogy nyaralásuk során, amennyiben nem megfelelően biztosított WIFI hálózaton

keresztül intézik céges ügyeiket, úgy nincsenek védve a hackertámadásoktól. Így minden vállalati, pénzügyi és személyes adat akadálytalanul juthat a támadók kezére. Javasolják, hogy a Virtual Private Network – Virtuális Magánhálózatot (VPN) vegyék igénybe, amely segítségével titkosítható a csatlakozó eszköz és a szerver között forgalom. 2016. szeptember 5-i hír, hogy kibertámadás érte a schwechati repülőteret. Az osztrák reptér igazgatója, Günther Ofner elmondása szerint rövid időn belül több irányból több támadás is érte a rendszert. Évek óta felkészültek egy hasonló incidensre, emiatt sikerült elhárítani a támadást. Feljelentést tett az osztrák belügyminisztériumnál, amely nyomozást indított az ügyben. Szerencsére nem fértek hozzá a támadók a repülőtér honlapjához, sem pedig a tárolt adatokhoz. Ebből a rövid válogatásból jól látni, hogy a hackerek világában semmi sem tűnik lehetetlennek és főképp nem tartanak szentnek és sérthetetlennek semmit, így a kiberbűnözésnek csak a kiberbűnözéssel szemben fellépő védelem szabhat határt.

4.5.2. Hackerekkel szembeni védelmi lehetőségek

A hackertámadások ellen tűzfallal, vírusvédelemmel, tudatos használattal és elővigyázatossággal védekezhetünk. Ugyanakkor a vállalatoknak, kormányzati hardvereknek nagyon félkészültnek kell lenniük ezzel a kérdéssel kapcsolatban. Miközben a mindennapos utazásaink, ügyeink intézései során egyre kevésbé érezzük magunkat biztonságban, a világban sorra történő és hazánkat is érintő események sorozatában, az interneten biztonságban véljük magunkat, vagy legalábbis biztonságosabbnak gondoljuk a virtuális világot a jelenkori valóságnál. Pedig nagyobb körültekintésre lenne szükség és elővigyázatosságra a kiber világban. Az interneten, a számítógépek világában nagyon sokrétűen épül fel a biztonság kérdése.

4.5.3 Az Anonymus hackercsoport, mint pozitív ügyért küzdő csoport

Az Anonymus hackercsoport egy olyan csoport, akik akár szimpatizánsokat is szerezhettek maguknak, tevékenykedéseik következtében. Támadásokat követtek el többek között drogkartell ellen, 2011-ben lekapcsolták a világ legnagyobb gyerekpornó-hálózatát, szintén ebben az évben szélsőjobboldali aktivisták ellen fordultak, illetve a 2015-ös párizsi Charlie Hedbo hetilap ellen elkövetett terroristatámadást követően háborút hirdettek az Iszlám Állam és az al-Kaida ellen, egy dzsihádista oldalt tettek elérhetetlenné néhány órára, 101 ezer Twitter-fiókot jelentettek és 5900 propagandavideót töröltettek. [10] Mindenkinek szíve joga eldönteni, hogy milyen mértékben szimpatizál az ilyen jellegű csoportok tevékenységeivel, ugyanakkor, ha egy magas fokú tudást jó ügyért használnak, úgy saját véleményem szerint elismerést érdemelnek.

4.5.4. Hacker, mint elismert foglalkozás

Úgy vélem, hogy amennyiben egy témával kapcsolatban érdeklődünk, akkor nyitott szemmel járunk-kelünk a világban, és észrevesszük az azzal kapcsolatos információt, óhatatlanul is szemet szúrnak mindennapjaink ténykedései közt is. Velem is így történt, amikor már tudtam, hogy az információs biztonság kérdésköre foglalkoztatja a fantáziám. Idén májusban keltette fel a figyelmem egy közterületen elhelyezett hirdetés, amely ilyen szöveggel futott: *„Új hivatása etikus hacker”.*

Alcím: *„Az élet túl rövid ahhoz, hogy egy unalmas állásban töltsd el.”*

Úgy gondolom, hogy az Y generáció szülötteivel kezdődően, a Z generáción át elképzelhető, hogy valaki etikus hacker foglalkozást űzzön. Mégis, talán az Alpha generáció jövője lesz ez igazán. De mit is jelent ez az etikus hacker kifejezés?A hirdetés feladója, a Deloitte globális hálózat, amely világszerte foglalkozik könyvvizsgálati, üzletviteli tanácsadási, pénzügyi tanácsadási, kockázati és adó-tanácsadási szolgáltatások biztosításával. Országszerte a helyi hatályos jogszabályoknak, más szabályozásnak, illetve a helyi gyakorlatnak és egyéb körülménynek megfelelő struktúrában működnek. Szolgáltatásaik sorában megtalálhatóak a következők: könyvvizsgálat és könyvvizsgálati tanácsadás, jogi szolgáltatás, üzletviteli tanácsadás, kockázatkezelés, pénzügyi tanácsadás, adó tanácsadás, üzleti folyamati tanácsadások és kutatás és fejlesztéssel is foglalkozik. Megbízhatóak, felkérhetők arra, hogy ellenőrizék a hálózatunkat, megfelelő-e az adatvédelmünk, kínál olyan szolgáltatásokat, amelyek segítségével az informatikai betörések esélye redukálható:

- **Sebezhetőségi vizsgálat:** ügyfeleink rendszerein észlelt biztonsági hiányosságok által okozott kockázatok felmérése
- **Infrastruktúra betörési tesztje:** az ügyfél kritikus hálózati infrastruktúráját érő hacker támadás szimulációja
- **Alkalmazás betörési tesztje:** alkalmazás biztonsági hibák felderítése, melyek jogosulatlan hozzáférést és tranzakciókat eredményezhetnek
- **Konfigurációellenőrzés:** a szerverek konfigurációjának ellenőrzése a gyenge pontok meghatározása érdekében
- **Kiberbiztonsági tanácsadás** [11]

Honlapjukon kínálnak állást pályakezdőknek ugyanúgy, mint tapasztalt munkavállalóknak. Modern az oldaluk, inspiratív felhívásokkal kecsegtet és könnyen átlátható, egy szóval profi.

Saját véleményem, hogy az informatikai szektorban ez a jövő. Hiszen a nagyvállalatoknak, energetikai szolgáltatóknak, reptereknek, állami hálózatoknak egyre fontosabbá fog válni a védelem biztosítása, mind a hacker csoportok kártékony támadásai ellen, mind a terroristák által elkövetett informatikai támadások ellen.

5. HÉTKÖZNAPI VESZÉLYEK AZ INFORMÁCIÓS BIZTONSÁG TERÜLETEIN

A Btk. 219. § Személyes adattal visszaélés

(1) Aki a személyes adatok védelméről vagy kezeléséről szóló törvényi rendelkezések megszegésével haszonszerzési célból vagy jelentős érdeksérelmet okozva

a) jogosulatlanul vagy a céltól eltérően személyes adatot kezel, vagy

b) az adatok biztonságát szolgáló intézkedést elmulasztja, vétség: 1 év.

(2) (1) aki a személyes adatok védelméről v. kezeléséről szóló tv-i rendelkezések megszegésével az érintett tájékoztatására vonatkozó kötelezettségének nem tesz eleget, és ezzel más v. mások érdekeit jelentősen sérti. [12]

Annak ellenére, hogy a Büntető Törvénykönyv elmarasztalja a személyes adattal való visszaélést, a mindennapok során számtalanszor kell óvatossággal eljárnunk, résen lennünk és kivédenünk a személyes adataink ellen irányuló támadásokat. A következő alfejezetben ezek közül ismertetek pár támadást.

5.1. Nyereményjátékok

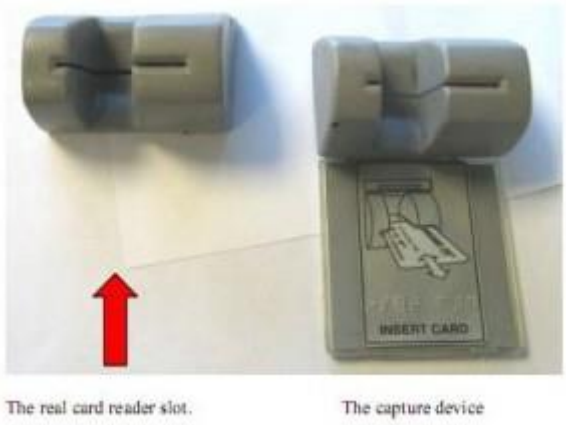
Rengetegen dőlnek be olyan nyereményjátékoknak, amelyeknek a valódi célja nem más, mint az adatszerzés. Természetesen kecsegtetőnek tűnik a pénzösszeg/autó/utazás vagy bármi más, amihez ingyen juthatunk hozzá, ugyanakkor ez az ingyen, valójában nincs ingyen. Hiszen az adatainkkal fizetünk a nyerési lehetőségért, amely ismerjük el eléggé csekély. Az adatainkat begyűjtik, tárolják és különböző módokon fel is használják. Vannak olyan átverések is, ahol valójában esélyünk sincs a nyeremény bezsebelésére, hiszen valótlan dologgal csábítják az információs biztonsággal kevésbé tudatos embereket. Például 2013-ban az egyik közösségi oldalon szereplő nyereményjátékban, a résztvevők elfogadták, hogy a személyes jellegű adataikat nyilvánosan közöljék, és a szervező használja reklám célra, területileg és/vagy időlegesen korlátozás nélkül, valamint bármilyen más módon (pl. internet, utcai felirat, stb.). Így, mindenkit óvva intek a hasonló meggondolatlan kattintásoktól és adatleírásoktól. Senki sem szeretné például egy felnőtteknek szóló hirdetés arcaként, arról való hamis „véleményt” közlő szereplőként viszontlátni magát az utcai óriásplakáton. Már üzletekben a vásárlást

követően megkapott blokkon is az adatgyűjtésre irányuló törekvéseket tapasztalhatunk. Személygépjármű, illetve pénzösszegnek a nyerési lehetőségére hívja fel a figyelmet a szöveg a blokkon, cserébe azt kéri, hogy névvel, telefonszámmal és lakcímmel ellátva dobjuk be a boltban elhelyezett gyűjtőládába a blokkot és így máris esélyessé válunk. Ezzel rendkívül hatásosan elérnek a Veterán generáció szülötteihez is, akik nagy valószínűséggel nem, vagy nagyon ritkán és limitáltan használják a világhálót. Nagyszüleim rendszeresen kapnak telefonhívásokat a lakásuk vezetékes telefonján, amely hívások során mindenféle egészségügyi eszközöket kívánnak értékesíteni. Az ilyen megkeresésektől el kell határolódni ahhoz, hogy biztonságban tudhassuk magunkat és a körülöttünk élőket.

5.2. Bankkártya adatok

Az emberek legtöbbje, ha a telefonszámát könnyedén meg is adja idegeneknek, amennyiben a bankkártya adataira terelődik a szó, már elutasítóvá válik, hiszen könnyedén lenullázható lesz a számlánk egyenlege, ha kiadjuk az erre vonatkozó adatainkat. Az üzletekben, amennyiben olyan bankkártyánk van, fizethetünk PayPass-al, azaz egy érintéssel. Ez a módszer 5000 Ft-os vásárlás esetén nem kér PIN kód beütést. Ez abból a szempontból kényelmes, hogy senki nem kukucskál át a vállunk felett, és lesi meg a PIN kódunkat. Ugyanakkor, ha ellopják a bankkártyánkat, bárki tud vele ötezer Ft alatt fizetni vele. Csak 5000 Ft feletti fizetés esetén kér PIN kódot a terminál, ahogy készpénzfelvételnél is. Készpénzfelvétel, illetve egyéb ATM művelet végrehajtásánál fokozottan figyelni kell, arra, hogy kellően takarjuk a gombokat, amikor beütjük a PIN kódunkat, hiszen szerelhetnek kis videó kamerát a csalók az ATM szerkezetére, abból a célból, hogy felvegyék kódunkat.

Egy internetes oldal [13] már évek óta foglalkozik a banki ATM-ekre specializálódott csalási eszközök ismertetésével. 2010-től egészen 2016-ig lopási történeteket, és be is mutatja az eszközöket, illetve, hogy mire kell figyelnünk.



2. ábra: Kártya mágnes csík leolvasó készülék [13]

A bal oldali az eredeti, a jobb oldali eszköz, egy olyan készülék, amely rá van pattintva az ATM eredeti kártyanyílására, és képes leolvasni a bankkártyán lévő mágnes csík adatait. Tartalmaz egy SMS küldő modult, így továbbítva az adatokat a tolvajnak.

4. ábra: ATM billentyűzet alatti figyelő [13]

A fenti képen egy ATM billentyűzet alatti billentyűzetfigyelő áramkör látható, mely különösen alkalmas PIN kódok kiolvasására. Az ál-billentyűzet kihajtva látszik, s a furfangos szerkezet visszapattintva természetesen átadja a billentyűnyomást a bankjegy-automata eredeti billentyűzetének is.

A cikkben még számos trükk megismerhető, például komplett kártyaszkennelő szerkezet, komplett ATM fedőlap modul (nem csak billentyűzet alatti figyelő, hanem az egész alkatrész), az SMS-t küldő áramkör továbbfejlesztett változata a Bluetooth-os adatkiküldő eszköz. Ennek hátránya a tolvajokra nézve, hogy a közelben kell lenniük, mivel rövid távolságon belül működik a Bluetooth. Ahogy fejlődik a technika, egyre elmésebbek lesznek a tolvajok is, és egyre kevésbé észrevehetően pici kamerákat szerelnek fel, illetve egyre jobban képesek leutánozni a tartozékok kinézetét, és felszerelni hamisakat az ATM-ekre.

Pénzügyeinkkel kapcsolatban nem csak az ATM-eknél és a boltban fizetésnél kell résen lennünk, hanem az internetes vásárlások során is oda kell figyelnünk. Hiszen mára már fizetéseink nagy része utalásokra korlátozódott, hiszen sokkal egyszerűbb beállítani egy-egy űrlapot az internetes bankfelületünkön, és automatizálni azt, illetve pár kattintással elintézni pénzügyeinket. Megkímél a sorban állástól, a várakozástól, ezáltal rengeteg időt spórolunk. Remek vásárlásokat is nyélbe lehet ütni az interneten, akár a hétköznapok során, de természetesen karácsony előtt számottevően megugrik az internetes vásárlások száma. Ilyen időszakokban a kártya adatok ellopásának bekövetkezése is magasabb százalékban fordul elő.

2011-ben több tízezer kártyatulajdonos kapott ilyen üzenetet bankjától: *"Biztonsága érdekében VISA kártyáján korlátoztuk a tranzakciókat. Az intézkedés nem érinti sem a belföldi vásárlást, sem az ATM készpénzfelvételt. Internetes és PIN nélküli külföldi vásárlási lehetőség - visszaélés gyanúja miatt - tiltásra került. Kártyáját ingyenesen cseréljük."* [14]

Több tízezer kártya adatai szivárogtak ki, egy külföldi elszámoló központból. 2009-ben a Heartland Payment System hozott nyilvánosságra egy hackertámadást, amelyet minden idők egyik legnagyobb számítógépes csalásának neveznek. Akkor körülbelül 130 millió bankkártya adatai kerültek a csalók kezébe. Szintén 2011-ben, áprilisban a Sony adatbázisából szerezték meg 77 millió felhasználó adatait, júniusban pedig a Citigroup jelentette be, hogy hackerek egy durva hibát kihasználva betörtek a rendszereibe, és ellopták több százezer bankkártya tulajdonos személyes adatát. Legyünk vele tisztában, hogy a nemzetközi kártyatársaságok sem e-mailben, sem telefonon nem keresik meg közvetlenül a kártyabirtokosokat, valamint e-mailben nem kérnek bizalmas adatokat, sem PIN kódot!

Online fizetés esetén minden győződjünk meg róla, hogy a kommunikáció titkosítva van-e; erre utal az URL címben a "https" valamint a mellette szereplő "lakat", melyre rákattintva meg kell jelennie a titkosításhoz használt tanúsítványnak. A világhálón előforduló lopási kísérletekkel szemben úgy lehetünk elővigyázatosak, hogy nyitunk a bankunknál egy úgynevezett PayPal számlát.

A PayPal definiálása a következő: *„A PayPal elektronikus számlát vezet ügyfelei részére, melyet azok hitelkártyás fizetéssel, banki átutalással vagy inkasszómegbízással tölthetnek fel lakossági vagy céges bankszámlájukról. Internetes vásárlások során nem kell bizalmas hitelkártya- vagy számlaadatokat megadni, ill. továbbítani, hanem a PayPal felhasználói név, valamint a jelszó megadása elegendő a fizetés lebonyolításához."*[15] Ezt az egyik magyar banknál Virtuális WEB Kártyának hívják, kizárólag elkülönített webKÁRTYA számlához kapcsolódhat, ezáltal a kártyával csak a webKÁRTYA számlán rendelkezésre álló összeg

erejéig lehet interneten vásárolni, így növelve az interneten történő vásárlás biztonságát. Érdemes utánanézni a bankunknál, hogy van-e lehetőség ilyen számla aktiválására, mert amennyiben ilyen keretek között vásárolunk az interneten, úgy biztosan védve vagyunk az internetes tolvajokkal szemben.

5.3. Mobiltelefon segítségével történő helymeghatározás

Az idén ősszel történt Teréz körúti robbantó elfogását szándékozom elemezni, információs biztonsági szempontok alapján. A bombát szétszedték és a benne levő áramkör alapján indultak el a rendőrök, amely szál elvezette őket a bolthoz, ahol az elkövető a vásárlást követően megadta az e-mail címét. Manapság már az e-mail fiókunk elérését telefonról is megtehetjük, ahogy naponta többször meg is tesszük. A budapesti merénylő is hasonlóan cselekedett, ez buktatta le, így tudták meg a tartózkodási helyét a nyomozók, a telefonja helymeghatározásának köszönhetően. A GSM telefon helyzetének meghatározását az teszi lehetővé, hogy általában több úgynevezett bázisállomás is látja a készüléket, és azt is többé-kevésbé pontosan lehet tudni, hogy milyen távolságra van ezektől a telefon. Ezekből az adatokból egyszerű matematikai műveletekkel meg lehet állapítani a mobil helyzetét. A pontosság attól függ, hogy milyen sűrűn vannak bázisállomások az adott területen. [16]

Ez a történet bárki mással lejátszható lenne, ugyanilyen formában. Egy e-mail cím, egy telefonszám alapján megállítható, hogy hol tartózkodik az illető.

5.4. Tömeges lehallgatások

A magyar mozikban már játsszák a Snowden című filmet, amely Edward Snowden történetét dolgozta fel. Edward Snowden a CIA informatikusa volt, ahol nyilvánvalóvá vált számára, hogy az amerikai Nemzetbiztonsági Ügynökség titokban amerikai telefonhívások millióit figyeli adatgyűjtés céljából, 9 jelentős internetszolgáltató szerverén végeztek adatgyűjtést, valamint állítólag létezett egy harmadik titkos adatgyűjtési program is, amelynek keretében hitelkártya-tranzakciók adatait rögzítették. Edward Snowden ezeket az információkat, bizonyítékokkal együtt kiszivárogtatta a The Guardian újságíróinak, ezt követően az egész világot bejárta a hír.

A leleplezést, s a folyamatosan kiszivárgó újabb és újabb részleteket komoly felháborodás fogadta, főleg Európában. Az amerikai illetékesek cáfolták, hogy tömegesen lehallgatták volna a telefonbeszélgetéseket, elolvasták volna az e-maileket: álláspontjuk szerint az átlagembereknek, akiknek nincs közük terroristákhoz, egyáltalán nincs mitől tartaniuk. Két évvel később, 2015-ben az amerikai szenátus elfogadta a képviselőház által kidolgozott Freedom Act tervezetét, ez a törvény vet véget a felhatalmazás nélküli tömeges adatgyűjtésnek.

A jogszabály értelmében már csak a telekommunikációs cégek gyűjthetik előfizetőik telefonhívásainak metaadatait - földrajzi hely, időtartam, résztvevők - az NSA csak meghatározott esetben, bírósági engedéllyel kérheti ki az adatokat. A törvény továbbá módosítja a külföldi hírszerzési-megfigyelési törvény (FISA) alapján történt adatlekéréseket - ez alapján kértek le információt a hatóságok egyebek közt a Facebook, a Google és a Twitter adatbázisából. Míg eddig amerikai állampolgárok ellen is folytathattak tömeges megfigyelést, addig az új törvény közösségi érdekvédőket rendelne az adatlekéréseket felügyelő titkos bíróság mellé. Feladatuk a magánélet védelmének biztosítása lenne, illetve a megfigyelések folyamatáról tájékoztatnák folyamatosan a bírákat.

A magyarországi szabályozás szerint a telekommunikációs cégek fél évig tárolják az előfizetőik forgalmi adatait. A hatóságok indoklás nélkül is tömegesen kérhetnek le adatokat, az előfizetők nem kérhetik adataik törlését, és nem is tájékoztatják őket ezek tárolásáról.

Ez a kérdés, főképp a növekvő terrorveszély hatására komoly vitákat szíthat. Mi a fontosabb, a védelem, amely melléktermék, hogy olyan információt is figyelnek és tárolnak rólunk, amely privát jellegű, netalántán a privát, magánélet védelme? Véleményem szerint erre hosszú évek múltán sem biztos, hogy kapunk választ. Az arany középutat lenne célszerű megtalálni, ám ki tudja oda húzni a határvonalat és milyen szempontok alapján? Ez a kérdés egyelőre maradjon költői és így megválaszolatlan.

6. VÉDELMI INTÉZKEDÉSEK

6.1. Az Európai Unió kiberbiztonsági stratégiája

Az Európai Unió Tanácsa létrehozott egy stratégiát, a kiberbiztonsági stratégiát, amelynek az a célja, hogy az európai telekommunikációs rendszerek meghibásodásait és az azok ellen indított támadásokat megelőzzék, illetve az ilyen esetekre kidolgozott válaszlépések kidolgozása. Az irányelvjavaslat az uniós tagállamokban alkalmazott minden digitális technológiára, hálózatra és szolgáltatásra vonatkozó minimális biztonsági szintet vezetne be. A javaslat bizonyos vállalkozások és szervezetek számára kötelezővé tenné a jelentős kiberbiztonsági események bejelentését is. Ezek közé tartoznak a keresőprogramokat és a számításifelhő-szolgáltatásokat kínáló szolgáltatók, a közösségi oldalak, a közigazgatási szervek, az online fizetést lehetővé tevő platformok (mint például a PayPal), valamint az Amazonhoz hasonló, jelentősebb internetes áruházak.

A stratégia a következő öt kiemelt terület kihívásaira adott válaszok tervezetét tartalmazza:

- a kibertámadásokkal szembeni ellenálló képesség megteremtése

- a kiberbűnözés drasztikus visszaszorítása
- az EU közös biztonság- és védelempolitikájához (KBVP) kapcsolódó kibervédelmi szakpolitika kidolgozása és kapacitás kiépítése
- a kiberbiztonság ipari és technológiai forrásainak fejlesztése
- a kibertérrel kapcsolatos kérdésekre vonatkozó koherens uniós nemzetközi szakpolitika kidolgozása

A javasolt intézkedések között jelen van, hogy:

- előírják a tagállamok számára egy Nemzeti Infokommunikációs Stratégia (NIS) kialakítását, valamint egy olyan nemzeti NIS-hatóság kijelölését, amelynek megfelelő erőforrásokkal kell rendelkeznie az ilyen kockázatok és események megelőzéséhez, kezeléséhez és az azokra adandó válaszlépések megtételéhez
- a tagállamok és a Bizottság közötti együttműködési mechanizmus kidolgozását szorgalmazzák, amely lehetővé teszi a kockázatokra és eseményekre vonatkozó korai riasztás megosztását, az információcserét és a NIS-fenyegetésekkel és -eseményekkel szembeni közös fellépést
- bizonyos digitális vállalatok és szolgáltatók számára előírják egy kockázatkezelési eljárás kidolgozását, illetve a komolyabb informatikai biztonsági események bejelentését az illetékes nemzeti hatóságnak.

A 2015. június 29-én tartott negyedik háromoldalú egyeztetés alkalmával a Tanács és az Európai Parlament megállapodott azokról az alapelvekről, amelyeknek be kell kerülniük a kiberbiztonsági irányelvtervezetbe. Véleményem szerint az Európai Unió kiberbiztonsággal kapcsolatos törekvéseit és rendelkezéseit célszerű lenne minden európai polgárnak ismernie. Kutatásom során külön kérdést szentelek ennek a témakörnek, hiszen foglalkoztat, hogy vajon hallotak-e erről a fogalomról az általam megkérdezettek, illetve tisztában vannak-e a stratégiában foglaltakkal? Előzetes feltevésem, hogy amennyiben hallottak róla a válaszadók, úgy e válaszolói személyek a fitalabb generációk szülöttei, hiszen az interneten valószínűsítem, hogy könnyebben találkoznak ezzel a kezdeményezéssel, mint azon kívül.

6.2. Az Európai Unió kiberbiztonsági szabályozásának ismertetése

Az Európai Parlament, 2015. december 8-án fogadta el az első közösségi szintű kiberbiztonsági szabályozást. A megállapodás jelentősen javítja az EU országainak kibervédelmi képességeit, illetve gördülékenyebbé teszi az erre irányuló tagállamok közti együttműködést. Az elfogadott szabályok az alapvető szolgáltatásokat nyújtó szolgáltatókra lesznek érvényesek, ilyenek

például az energia, a közlekedési, a banki és az egészségügyi ágazatok résztvevői, valamint az olyan digitális szolgáltatást nyújtó szolgáltatók, mint a kereső motorokat és a felhő alapú szolgáltatásokat működtető szervezetek. Ezeknek a kiemelt szereplőknek meg kell tenni a megfelelő biztonsági intézkedéseket, valamint jelenteniük kell a különleges eseményeket az illetékes nemzeti hatóságoknak. Az információs rendszerek egyre nagyobb biztonsági kihívásokkal kénytelenek szembenézni: a rosszindulatú támadások mellett a műszaki és nem szándékos hibák, a természeti csapások mind-mind potenciális veszélyforrásoknak minősülnek. Ennek megfelelően az ilyen rendszereken keresztül az olyan alapvető és létfontosságú szolgáltatások is megzavarhatók, mint a víz-, a villany-, vagy épp az egészségügyi ellátás, de akár a közlekedési rendszer is.

A Bizottság számára az egyik legfőbb szempont, hogy segítsen megelőzni az ilyen jellegű eseményeket, azonban, ha mégis bekövetkezne, akkor a leghatékonyabb választ tudja rá adni. Ebből az okból kifolyólag a Bizottság már 2013-ban előterjesztette a hálózat- és információbiztonságra vonatkozó irányelvjavaslatát (NIS irányelv) az Európai unióban.

Az Európai Parlament és a Tanács képviseletében a luxemburgi elnökség által elfogadott megállapodás a következő kötelezettségeket tartalmazza:

- javítani kell a tagállamok kibervédelmi képességét
- javítani tagállamok közötti együttműködést a kiberbiztonság területén
- elfogadott szabályok az alapvető szolgáltatásokat nyújtó szolgáltatókra lesznek érvényesek, ilyenek például az energia, a közlekedési, a bankszektor szereplői, valamint az egészségügyi szolgáltatást nyújtók, valamint az olyan digitális szolgáltatást nyújtó szervezetek, mint a kereső motorokat és a felhő alapú szolgáltatásokat működtető vállalatok. [18]

6.3. A kibertér képviselőinek világkonferenciája

Világkonferencia a kibertér biztonságának érdekében hírére kettős gondolatok születnek meg bennem, hiszen egyfelől megnyugtató az indítvány, másfelől pedig maga az esemény megmutatja, hogy milyen szinten kell foglalkozni ezzel a témával. Bizonyítja, hogy szükség van védelemre, tudatosan óvatosan cselekvő felhasználókra a mindennapokban. A világkonferencia kezdeményezése 2011-be, azóta minden évben a kormányzatok, a magánszektor és a civil társadalom képviselői összegyűlnek, annak érdekében, hogy elősegítsék a gyakorlati együttműködést a virtuális térben, a számítógépes kapacitás kiépítésének fokozását, valamint, hogy megvitassák a virtuális térben elvárható normákat, a

felelős magatartás ismérveit. A 2011-es, első konferencia Londonban volt, ahol meghatározták a kibertérben elvárható, irányadó viselkedést.

Budapesten tartották a második konferenciát, 2012 októberében, amikor is a fő téma az internetes jogok és az internet biztonsága közötti kapcsolat volt. Pályaművek készítésének fő témái voltak a kibertér biztonsága, szabadsága, illetve a gazdasági-társadalmi jólét növelése.

2013-ban Szöulban került megrendezésre az esemény, amely során kiemelésre került annak fontossága, hogy egyetemes internetkapcsolat legyen a világon, és hangsúlyozásra került az online jogok védelme.

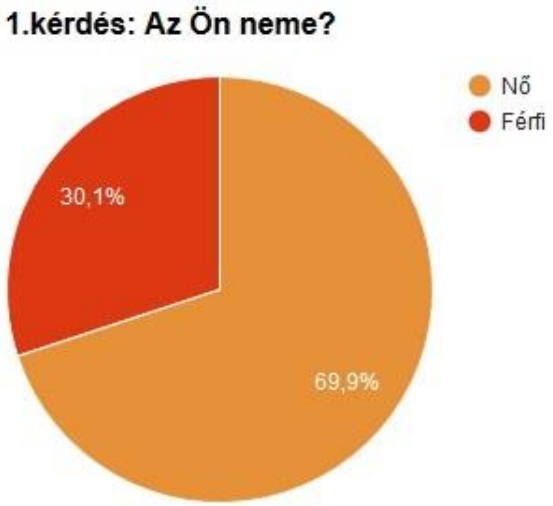
7. KUTATÁSI EREDMÉNYEK ISMERTETÉSE

Vizsgálati minta bemutatása és a vizsgálat elemzése

A kérdőívet, amely a ma élő hat generáció információs biztonsággal és védelemmel kapcsolatos hozzáállását kutattam 2016. szeptember 20-tól október 13-ig 163 válaszadó töltötte ki, Google Kérdőív formátumban, interneten keresztül. A kérdőív kérdéseit a dolgozatom mellékleteként csatoltam. Ez a kérdőív 15 kérdésből állt, s az eredményeit a továbbiakban be fogom mutatni, valamint elemezni fogom azokat.

Férfi és nő válaszadók aránya

Elsöprő arányban voltak a női válaszadók, hiszen a 163 válaszadó 69,9%-a volt hölgy, és mindössze 30,1 % férfi válaszolt a feltett kérdésekre.



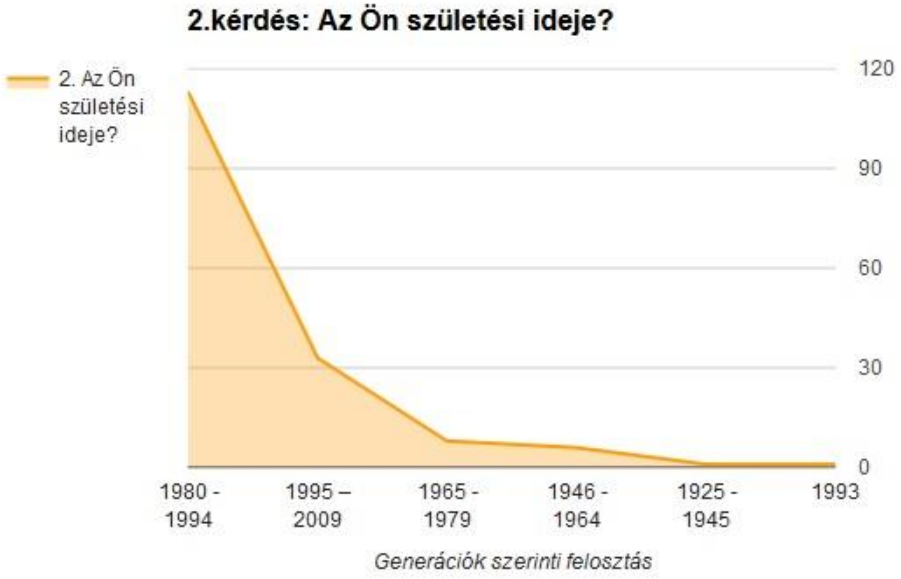
3. ábra: A nemek eloszlása [20]

A válaszadók közül kimagasló arányban a hölgyek voltak, amely eredmény összevetve a második kérdésre érkezett válaszok arányaival, nem áll összhangban a KSH 2011-es kutatásával. Természetesen elképzelhető, hogy 2011 óta jócskán változott a nemek aránya az adott korcsoportokban, illetve az is lehetséges, hogy az általam elért emberek túlnyomó része hölgy volt, továbbá feltételezésem szerint a hölgyek szívesebben töltenek ki teszteket, mint a férfitársaik

2. táblázat: 2011: nemek eloszlása korcsoport szerint [21]

A népesség korcsoport és nemek szerint KSH 2011			
Korcsoport	**Férfi**	**Korcsopor**	**Nő**
20–24	317 039	20–24	301196
25–29	310 238	25–29	301063
30–34	385 903	30–34	379414
35–39	412 285	35–39	403311

Generációs arányok



4. ábra: Generációk szerinti felosztás [20]

A második kérdés segítségemre volt abban, hogy rögtön be tudjam sorolni a válaszadókat a generációk soraiba. Látható, hogy 114 válaszadó tartozik az Y generáció (1980-1994) közé, amely arány nem okoz meglepetést, hiszen jómagam is e generáció szülötte vagyok, így az

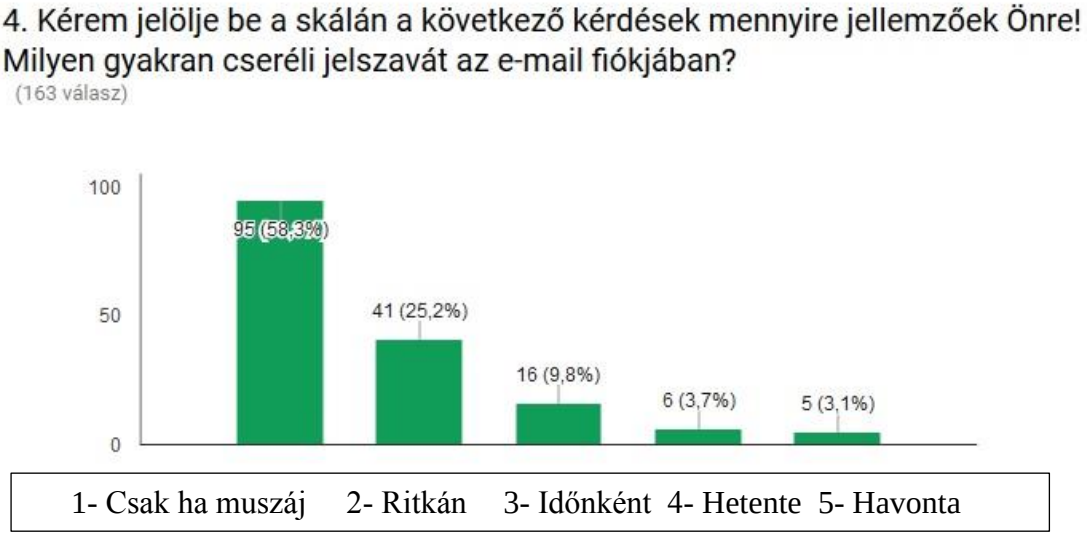
általam elért ismeretségi kör nagy részét a generációs társaim alkotják. Szintén az internetet legaktívabban használók között is jelentősen képviseli magát az Y generáció. Rögtön utánuk következik a Z generáció, akárcsak a való életben az Y generációt követi az 1995-2009 születettek sora. Ők 20,2%-a voltak a válaszadó személyeknek. 8 ember képviseltette magát az X generáció (1965-1979) szülöttei közül, a II. világháborút követő népességrobbanás gyermekei, a Baby Boom generáció (1946-1964) szülöttei közül 6 ember adott választ a kérdőívemben feltett kérdésekre. Egy személyben képviselte magát a kérdőív kitöltői között a Veterán, azaz csendes generáció (1925-1945), amely a világháborút megélt generáció. Az Alpha, vagy Új csendes generáció, a 2010 után született gyermekek közül egy sem adott választ a kérdőívre, természetesen egy hat éves gyermek számára nem releváns ilyen kérdések megválaszolása.

Iskolai végzettség

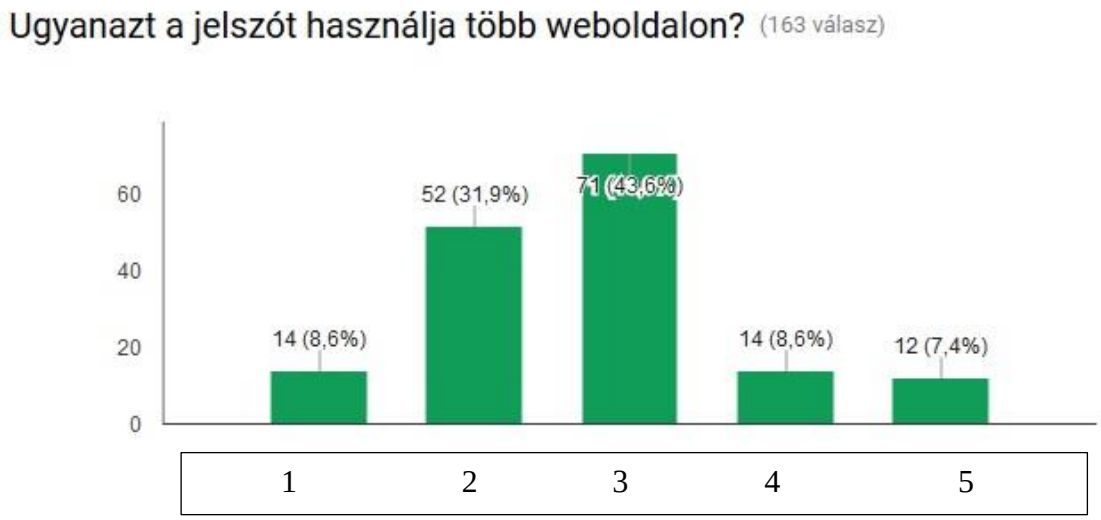
A kérdőívemben feltett kérdések közül a harmadik kérdés a legmagasabb iskolai végzettségről szólt, a válaszadók közül 51 személy rendelkezik egyetemi diplomával, érettségivel 46 személy, és 32 válaszadónak felsőfokú szakképesítés a legmagasabb iskolai végzettsége. Főiskolai végzettséggel a válaszadók 17% rendelkezik. Szakközépiskolai végzettséggel hatan adtak választ, illetve doktori végzettségű ember nem volt a válaszadók között. Egy női válaszadó volt, aki 1995 – 2009 között született és általános iskolát jelölt be, mint legmagasabb iskolai végzettség.

Az alapkérdéseket követően 3 lineális skála típusú kérdést tettem fel, amelyek megválaszolása szintén kötelező kérdésként szerepelt. Az 1 és az 5 közötti értékek értelem szerűen növekvő sorrendként szerepeltek, míg az 1-es jelentése a kötelező, az 5-ös érték jelentése a gyakran, szinte mindig volt, mindegyik kérdés esetében.

E-mail jelszavakkal kapcsolatos kérdések



5. ábra: E-mail fiók jelszócseréjének gyakorisága [20]



6. ábra: Azonos jelszavak használata [20]

1– Mindenhol ugyanaz a jelszavam

2- Számos helyen megegyező

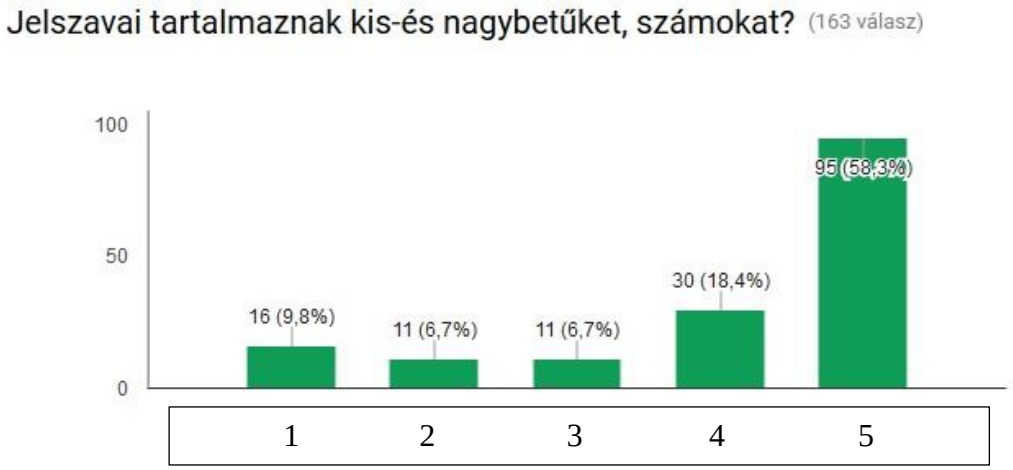
3- Nem jellemző

4- Ritkán

5- Soha nem használok kétszer ugyanolyan jelszót

E lineáris skálás kérdés eredményeképpen átlagosnak nevezhető a jelszavak variálása különböző webes felületek keretében. A válaszadók 44%-ra nem jellemző, hogy ugyanazt a jelszót használja több weboldalon. 14 embernek minden weboldalon megegyező a jelszava, amellyel regisztrál és 12 ember soha nem használja kétszer ugyanazt a jelszót, tehát minden felületen különböző jelszóval regisztrál. 52 válaszadó használ számos helyen megegyező jelszavakat, és 14 ember ritkán ad meg ugyanolyan jelszavat több helyen.

A harmadik lineáris skálás kérdésemre meglepetéssel konstatáltam, hogy a válaszadók több mint fele, 53%-uk mindig odafigyel arra, hogy jelszavuk tartalmazzon kis-és nagybetűket, valamint számokat.

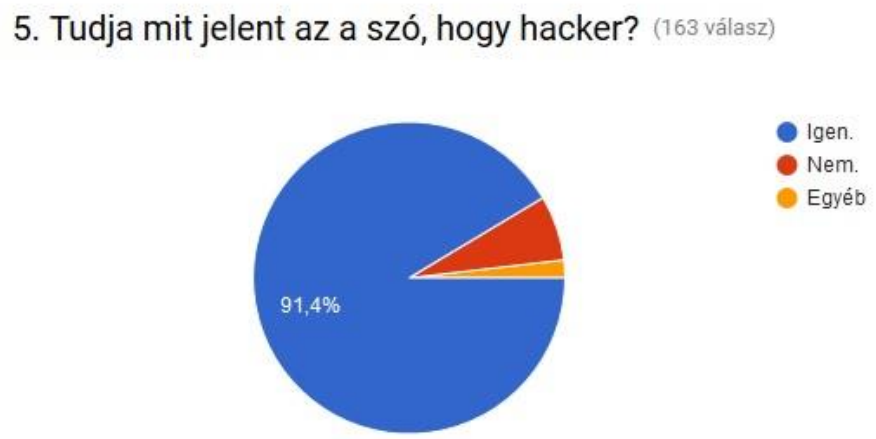


7. ábra: Jelszavak kis-és nagybetűk, számok arányának tartalmazása [20]

Mindössze 16 ember csak akkor figyel erre oda, amennyiben az adott weblapon a regisztrációhoz kötelezővé teszik ezek megadását. Véleményem szerint ez tükrözi a válaszadók, amely túlnyomó részt az Y és a Z generáció szülöttei tudatos hozzáállását a jelszóvédelem fontosságához. Napjainkban egyre gyakoribb az e-mail fiókok, egyéb oldalak jelszavainak feltörése, így szükséges, hogy regisztrációnk során bonyolult karaktereket megadva csökkentsük annak veszélyét, hogy fiók feltörés áldozataivá, illetve adathalászok, adatlopás áldozataivá váljunk.

Hackerekkel kapcsolatos ismeret

Következő kérdésem arra vonatkozott, hogy megtudjam tisztában vannak-e a válaszadók a hacker fogalom jelentésével. A válaszadók közül 149 ember tisztában van, válaszuk alapján a hacker kifejezés jelentésével. Csak 11 válaszadó nem tudja biztosan mit is jelent a szó. Ezt követően megkértem a kitöltőket, hogy opcionálisan, amennyiben tisztában vannak a hacker szó jelentésével, legyenek kedvesek leírni azt.



8. ábra: Hacker kifejezés ismeretének aránya [20]

Miután a válaszadók ilyen kimagasló arányban tisztában voltak, a hacker kifejezés jelentésével, áttanulmányoztam a pontos megfogalmazásukat arra vonatkozóan, hogy mit is jelent. Valóban, a nem kötelező kérdésre válaszolók (124 személy) közül 97%-uk tisztában van a hacker szó jelentésével, ennek bizonyításául bemutatok pár választ:

- „A hacker kifejezés alatt olyan számítástechnikai szakembert értünk, aki bizonyos informatikai rendszerek működését a publikus vagy a mindenki számára elérhető szint fölött ismeri. Ezek a szakemberek a számítástechnika egy vagy több ágát rendkívül magas szinten művelik, nagyon gyakran ők azok, akik „létrehozzák" azokat az eljárásokat, amik alapján a számítógépek vagy a hálózatok működnek." *Nő válaszadó, Y generáció, érettségi*
- „Számítástechnikában jártas ember, aki azon képességét, hogy ismeri ezeket a rendszereket akár bizalmas, titkos, személyes vagy csak fontos információk megszerzésére is használhatja." *Nő válaszadó, Z generáció, érettségi*
- „Olyan számítástechnikai szakember, aki bizonyos informatikai rendszerek működését a publikus vagy a mindenki számára elérhető szint fölött ismeri." *Férfi válaszadó, Y generáció, felsőfokú szakképesítés*

- „Virtuális "bűnöző", aki olyan adatokhoz szerez hozzáférést, amihez nincs joga.” *Nő válaszadó, Z generáció, érettségi*

A 163 megkérdezett közül 43% van azon a véleményen, hogy a mindennapi felhasználóknak átlagosnak mondhatón okuk van félni a hackerek tevékenységeitől. 21 ember szerint valós félelemre adnak okot a hackerek tevékenységei, a mindennapi felhasználók életében. 6 ember véli úgy, hogy egyáltalán nem szükséges tartania egy mindennapi felhasználónak a hackerek támadásaitól. A hackerek tevékenységei számos kiberbűnözési szinten megjelenhet, így egy terrortámadás is megtörténhet, például repülőgép eltérítés, nemzetbiztonsági adatok eltulajdonítása és azokkal való visszaélés megtörténhet a tevékenységeik kapcsán.

Terrortámadások és informatikai biztonság összefüggése

9. ábra: Terrortámadások és informatikai biztonság [20]

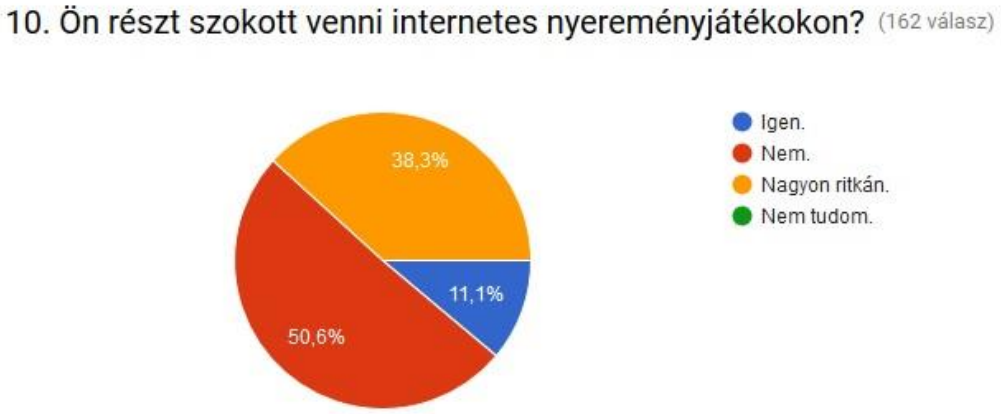
98 válaszadó határozottan azon az álláspontonvan, hogy szükség van a nagyobb odafigyelésre az informatikai biztonság területein is, az elmúlt idők terroreseményeinek hatására. A válaszadók 23% -a bizonytalan a kérdéssel kapcsolatban. Kizárólag 28 személy vélte úgy, hogy nem szükséges jobban ügyelni az informatikai biztonsággal kapcsolatos kérdésekre, vagyis a terrorcselekmények elkövetésének szaporodása nem figyelmeztet arra, hogy tudatosabbá kellene válnunk az online térben.

Az Európai Unió kiberbiztonsági stratégiájával kapcsolatos tájékozottság

10. ábra: EU kiberbiztonsági stratégiájának ismerete, mint fogalom [20]

Megdöbbentően magas az az arány, 163 válaszadónak 47%-a, még soha nem hallott az Európai Unió kiberbiztonsági stratégiájáról. A válaszadók közül 38%, hallott már róla, de nem tudja, hogy pontosan mit jelent ez a fogalom. A megkérdezett 163 ember közül kizárólag 14 ember hallott az Európai Unió kiberbiztonsági stratégiájáról úgy, hogy tisztában is van a tartalmával.

Nyereményjátékokon való részvétel aránya

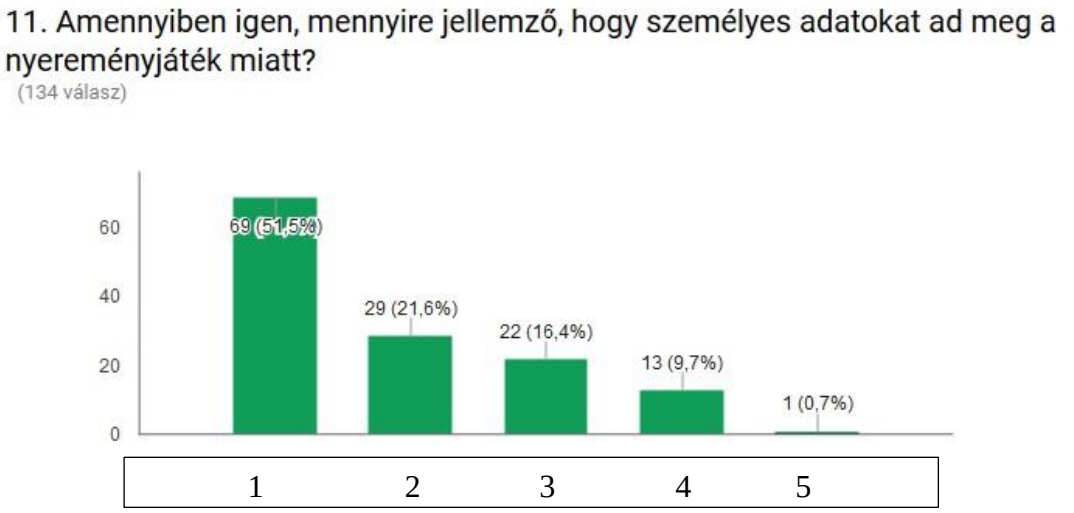


11. ábra: Nyereményjátékokon való részvételi arány [20]

A válaszadók 50,6% egyáltalán nem szokott részt venni nyereményjátékokon. 38,3%-uk pedig nagyon ritkán. 18 ember válaszolt igennel a kérdésre.

Személyes adatok megadása

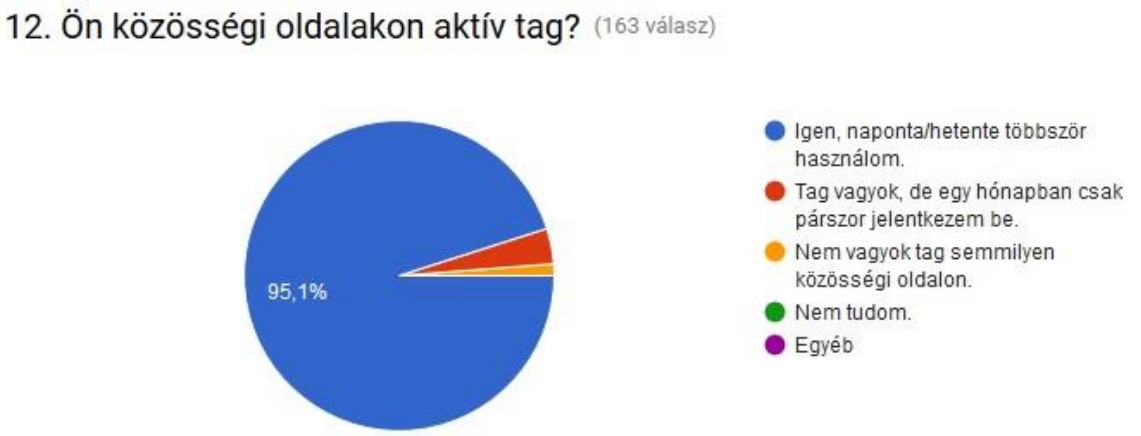
Tovább vizsgálva a nyereményjátékos kérdéskört kíváncsi voltam arra, hogy amennyiben részt vesznek ilyen jellegű dologban, megadnak-e személyes adatokat a kérdőív kitöltői?



12. ábra: Személyes adatok megadásának gyakorisága, nyereményjátékban való részvétel során [20]

69 válaszadó jelezte, hogy „soha nem ad meg személyes adatokat, nyereményjátékok kedvéért, akkor inkább nem vesznek benne részt", ahogy ez az első oszlopról leolvasható. 22%-a a válaszadó időnként megad személyes adatokat, azért hogy részt vehessen egyes nyereményjátékokon. Kizárólag egy válaszadó jelezte, hogy gond nélkül megadja az adatait, ő egy Y generációs hölgy volt.

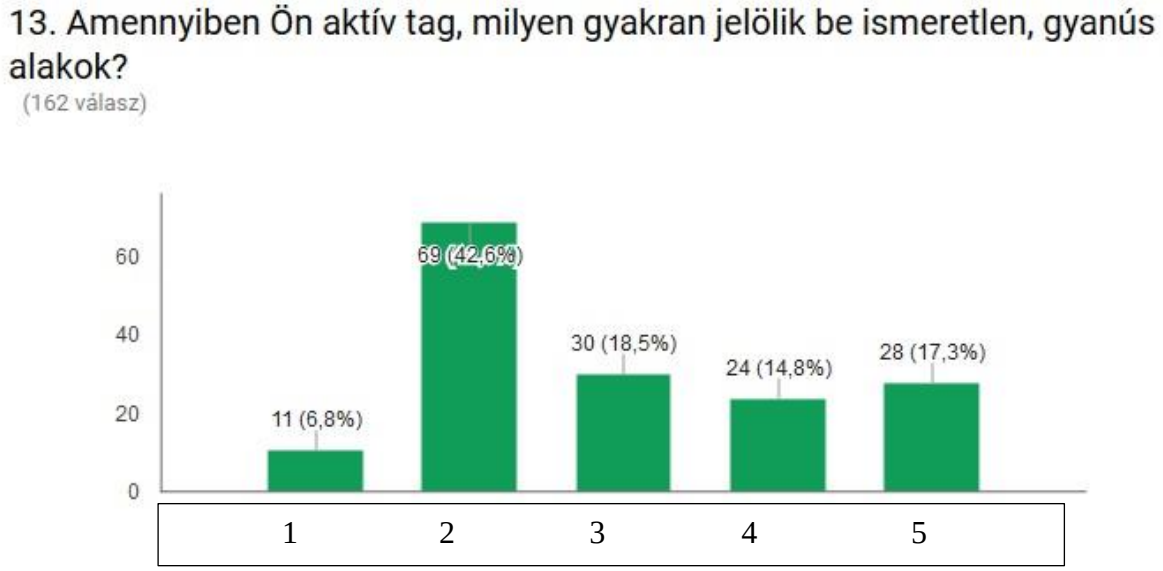
Közösségi oldalakon való aktivitás



13. ábra: Közösségi oldalon való aktivitás aránya a megkérdezettek körében [20]

Kimagasló a napi szinten közösségi oldalakat használók tömege, 95%-uk a válaszadóknak, bevallom én is ezek közé tartozom. A megkérdezettek közül ez pontosan 155 embert jelent. A havonta ritkán közösségi oldalra bejelentkezők aránya 3,7%, és mindössze 2 válaszadó egyáltalán nem regisztrált tag semmilyen közösségi oldal felületén.

Idegenek közeledése a közösségi oldalakon



14. ábra: Közösségi oldalon idegen, gyanús személyek közeledése a válaszadók felé [20]

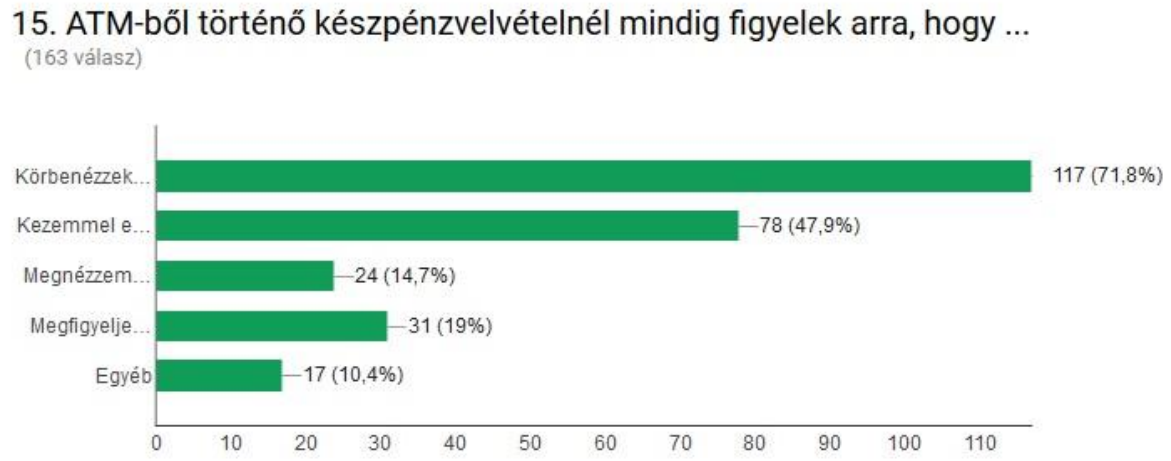
A 163 válaszadó 43%-a jellemzően nem találkozott még, ilyen jellegű közeledéssel. 11 emberrel egyáltalán nem fordult elő, hogy idegen, kétes küllemű személy ismerősnek jelölte volna. A 3, 4 és az 5 pont nagyjából megegyező értékeket mutat, tehát összegezhető, hogy ez egy előforduló jelenség, habár nem kiemelkedően egyértelműsíthető, hogy gyakran megtörtént a válaszadók körében, átlagosnak mondható a kétes személyek közeledése a közösségi oldalakon, a napi szinten aktív Y és Z generációs felhasználók között. Magától érthetődő számomra az a kérdés, hogy amennyiben előfordul ilyen jellegű személy közeledése, azt elfogadják-e a válaszadók, így következő kérdésem erre vonatkozott.

Ön visszajelölte ismerősnek ezek a személyeket?

15. ábra: Gyanús személyek ismerősi felkérésnek elfogadásának aránya [20]

91%-a a válaszadóknak, számszerűsítve 148 személy egyáltalán nem fogadja el az idegen, kétes alakoktól induló ismerősi felkéréseket. E kérdés megválaszolásánál 10 ember nem találkozott még ilyen jelenséggel. Kizárólag 2 ember volt azon a véleményen, hogy semmi akadályát nem látja a felkérés elfogadásának, tehát 91%-an nem jelölték vissza ismerősnek az idegen személyeket, a közösségi oldalakon.

Amire a legtöbben odafigyelnek készpénzfelvétel során



16. ábra: ATM-nél történő kézpénzfelvétel biztonsági körülményeire való odafigyelés [20]

E kérdés megválaszolásánál több opciót is bejelölhettek a válaszadók. 117 személy mindig körbenéz, megfigyelve, hogy nem álltak-e túl közel hozzájuk idegen személyek. 78 ember minden alkalommal eltakarja a PIN kód beütésénél a számlapot. A csalók eszközei közül

leggyakrabban használt mágnescsík leolvasó készülék és a hamis ATM billentyűzet közül, a válaszadók gyakrabban figyelnek oda a bankkártya mágnescsík leolvasó készülék jelenlétére. 31 ember figyeli meg rendszeresen kézpénzfelvételnél a hamis leolvasó készülék ottlétét, és 24 személy sok esetben fordít odafigyelést a billentyűzet szemrevételezésére. A kitöltők közül 17 érintett adott meg egyéb választ, amelyeket a továbbiakban ismertetek. A 17 személyből 11 ember adott értelmezhető, egyéb szöveges választ a kérdésre. Közülük 8 ember az Y generáció szülötte, 4 nő és 4 férfi. Három személy mindegyik megadott lehetőségre figyel a fentiek közül. Két ember egyáltalán nem foglalkozik egyik opcióval sem. Az Y generációs kitöltők közül két személy pedig soha nem vesz fel pénzt ATM-ből, egy válaszadó általában csak egy helyről szokott pénzt felvenni, amiről tudja, hogy biztonságos. Két X generációs személy egy nő és egy férfi közül a főiskolai végzettségű férfi mindegyik veszélyforrásra figyelmet fordít és csak ismerős ATM-ből vesz fel kézpénzt. Az X generációs hölgy válaszadó pedig egyáltalán nem használ ATM-et. Az egyetlen Veterán generációba tartozó főiskolai végzettséggel rendelkező kitöltő, válasza alapján mindegyik lehetőségre egyformán odafigyel.

8. ÖSSZEGZÉS

Dolgozatomban az információs biztonság témakörének komplex értelmezését követően, amely a megfelelő szakirodalmak áttanulmányozása után került tisztázásra, ismertettem a ma élő hat generáció besorolására vonatkozó szempontokat, és a rájuk jellemző adatokat. A 163 emberrel kitöltetett kérdőíves vizsgálat eredményeit összevetve, a megkérdezettek nagy része, bizonyos helyzetekben tudatosan, megfontoltan használja mindennapok során az online felületen elérhető oldalak kezelését. Kérdőívemre az Y generáció és a Z generáció szülöttei válaszoltak a legtöbben, ebből azt a következtetést szűröm le, hogy az interneten keresztül őket lehet a legkönnyebben elérni. Szintén ők a legaktívabb felhasználók a közösségi oldalakon.

Ismertettem a munkám elkészítése során a virtuális világban előforduló főbb veszélyeket, amelyek a hétköznapi felhasználókra leselkednek, mindennap internet használat során. Az ezzel kapcsolatos kérdőívkérdések kielemzését követően kijelentem, hogy jelszóvédelem tekintetében a csere, nem igazán jellemző a felhasználókra, ugyanakkor megállapítható, hogy nem használják számos helyen ugyanazt a jelszót, amely tudatos odafigyelésre vall. Az általuk megadott jelszavak karakterisztikus tulajdonságai pedig elsöprő odafigyelésről tesznek tanúságot, az Y és a Z generáció szülöttei között. Tehát a jelszavak beállításának és használatának tekintetében tudatosnak mondhatók a megkérdezettek. Megállapítom, hogy a megkérdezettek 91%-a tisztában van a hacker fogalom jelentésével, és

azzal is, hogy mivel foglalkoznak, ugyanakkor a válaszadók 19%-a gondolja azt, hogy a hétköznapi felhasználónak nincs oka tartani a hackerek tevékenységétől. A kitöltők 60%-a vallja azt, hogy a megnövekedett terrortámadások hatására jobban oda kellene figyelni az informatikai biztonsággal kapcsolatosan felmerülő esetleges veszélyforrásokra. Az Európai Uniós kiberbiztonsági stratégia az ilyen jellegű veszélyek kiküszöbölése érdekében született meg. A válaszadók közül mégis, kizárólag 14 ember hallott az Európai Unió kiberbiztonsági stratégiájáról úgy, hogy tisztában is van azzal, hogy mit tartalmaz maga a stratégia. Az internetes, nyereményjátékokon a válaszadók fele nem szokott részt venni, amely tudatos odafigyelésre enged következtetést levonni, hiszen egyáltalán nem jellemző a válaszadókra, hogy személyes adatokat adjon meg egy nyeremény játék során. A válaszadók fele mindennap, vagy hetente aktív felhasználója valamilyen közösségi oldalnak. A kitöltők között 42%-ban csak alig párszor fordult elő, hogy ismeretlen, gyanús emberek, ismerősnek jelölte volna őt, valamely közösségi oldal felületén, és a megkérdezettek 91%-a nem is fogad el ilyen jelöléseket. Konklúzióm, hogy a ma élő hat generáció tudatosan odafigyel az információs biztonsággal kapcsolatos mindennapos tevékenységek során. Az Y és a Z generáció szülöttei igenis tudatosan vannak jelen a közösségi oldalakon és egyéb felhasználói felületeken, odafigyelnek a jelszavaik védelmére, a személyes adataik titoktartására, valamint körültekintéssel vannak azzal kapcsolatban, hogy olyan személy ne váljon ismerősükké, akit valójában nem ismernek.

Ugyanakkor lényeges következtetést vonok le abból az eredményből, miszerint a megkérdezett 163 ember közül kizárólag 14 ember hallott az Európai Unió kiberbiztonsági stratégiájáról úgy, hogy tisztában is van a tartalmával. Ez aggodalomra adhat okot, hiszen az online tér biztonsága, az információ biztonság, az online fizetéssel kapcsolatos platformok biztonsága, a mindennapi életünket átfogó információhalmaz biztonságának védelme nagyobb figyelmet érdemelne. Maga a stratégia megalkotása, kidolgozása és elfogadása, valamint betartása rendkívül nagy pozitívum, ugyanakkor az emberek tájékoztatása és e stratégiával való megismertetése elengedhetetlen ahhoz, hogy optimálisan tudják használni és alkalmazni azt. Javasolnám az Európai Uniós kiberstratégia pontjainak terjesztését, például társadalmi célú hirdetés formájában, hogy megismerhessék a mindennapi felhasználók annak tartalmát.

Irodalomjegyzék

[1] Dr. Haig, Zs. (ismeretlen dátum): Az információbiztonság komplex értelmezése 1-4.o.

[2] Ismeretlen szerző (ismeretlen dátum): Az informatika hatása az emberi kapcsolatokra http://tudasbazis.sulinet.hu/hu/informatika/informatika/informatika-6-evfolyam Letöltés ideje: 2016.09.07.

[3] Ismeretlen szerző (2009): Digitális szakadék a generációk között, 2009 http://eduline.hu/kozoktatas/2009/2/3/20090203_digitalis_szakadek Letöltés ideje: 2016.09.07.

[4] Kissné András K. (2014): Generációk, munkaerőpiac és a motiváció http://munkajog.hu/rovatok/napi-hr/generaciok-munkaeropiac-es-a-motivacio Letöltés ideje: 2016.09.13.

[5] Kissné András K. (2014): Generációk, munkaerőpiac és a motiváció http://munkajog.hu/rovatok/napi-hr/generaciok-munkaeropiac-es-a-motivacio Letöltés ideje: 2016.09.13.

[6] Kulcsár L. (2011): Norton-jelentés: a család a netre költözött –félteni való gyerekek http://infovilag.hu/hir-22380-norton_jelentes_csalad_netre_koltozott_f.html Letöltés ideje: 2016.09.13.

[7] Al Qa'idy A.A.: A Course in the Art of Recruiting http://ia600300.us.archive.org/32/items/ACourseInTheArtOfRecruiting-RevisedJuly2010/A_Course_in_the_Art_of_Recruiting_-_Revised_July2010.pdf Letöltés ideje: 2016.09.14.

[8] Serdült V. (2015): A világon csak két dolog biztos: a halál és a kiberbűnözés http://www.origo.hu/techbazis/20150420-a-vilagon-csak-ket-dolog-biztos-a-halal-es-a-kiberbunozes.html Letöltés ideje: 2016.09.07.

[9] hvg.hu (2016): Telepítse a gépére: minden letiltott weboldalt elérhet, ha ezt használja http://hvg.hu/tudomany/20160426_betternet_google_chrome_bovitmeny Letöltés ideje: 2016.09.14.

[10] Halász Á. (2012): Ők az Anonymous – interjú a hackermozgalom magyar csoportjával http://www.mohaonline.hu/eszme/anonymous_hacker_mozgalom_magyar_interju Letöltés ideje: 2016.09.14.

[11] Deloitte (2016): http://www2.deloitte.com/hu/hu/pages/kockazat/solutions/sebezhetoseg-betoresi-tesztek.html Letöltés ideje: 2016.09.14.

[12] Btk. 219. § Személyes adattal visszaélés http://buntetojog.info/kulonos-resz/btk-219-%C2%A7-szemelyes-adattal-visszaeles/ Letöltés ideje: 2016.09.14.

[13] Word Press (2016): All About Skimmers: https://krebsonsecurity.com/all-about-skimmers/ Letöltés ideje: 2016.09.14.

[14] Ismeretlen szerző (Ismeretlen dátum): Még tombol az év bankkártya-botránya: http://m.portfolio.hu/finanszirozas/bankok/meg_tombol_az_ev_bankkartya-botranya.160528.html Letöltés ideje: 2016.09.14.

[15] PayPal fogalma https://hu.wikipedia.org/wiki/PayPal Letöltés ideje: 2016.09.09.

[16] Techline.hu (2016): Mérje be a mobilját – vagy valaki másét! http://hvg.hu/tudomany/20071015_nyomkovetes Letöltés ideje: 2016.10.22.

[17] A kiberbiztonság javítása az Európai Unióban http://www.consilium.europa.eu/hu/policies/cyber-security/ Letöltés ideje: 2016.09.19.

[18] Biztosítási Szemle: Elfogadták az EU kiberbiztonságra vonatkozó szabályozást (2016): http://www.biztositasiszemle.hu/cikk/nemzetkozihirek/eu/elfogadtak_az_eu_kiberbiztonsagara_vonatkozo_szabalyozast.5366.html Letöltés ideje: 2016.09.19.

[19] GCCS (2016): About the Global Conference on CyberSpace 2015 https://www.gccs2015.com/gccs/all-about-gccs2015 Letöltés ideje:2016.09.12.

[20] Saját készítés

[21] Népszámlálás 2011: Országos adatok: A népesség korcsoport és nemek szerint http://www.ksh.hu/nepszamlalas/tablak_teruleti_00 Letöltés ideje: 2016.10.14.

Ábrajegyzék

A **kérdőíves kutatás kérdései**

1. Az Ön neme?

- Férfi
- Nő

2. Az Ön születési ideje?

- 1925 – 1945
- 1946 – 1964
- 1965 – 1979
- 1980 – 1994
- 1995 – 2009

3. Legmagasabb iskolai végzettsége?

- Általános iskola
- Általános iskola
- Érettségi
- Felsőfokú szakképesítés (OKJ)
- Főiskola
- Egyetem
- Doktori

4. Kérem jelölje be a skálán a következő kérdések mennyire jellemzőek Önre! (1 2 3 4 5)

- Milyen gyakran cseréli jelszavát az e-mail fiókjában?
- Ugyanazt a jelszót használja több weboldalon?
- Jelszavai tartalmaznak kis-és nagybetűket, számokat?

5. Tudja mit jelent az a szó, hogy hacker?

- Igen
- Nem

6. Amennyiben igen, kérem írja le!

……

7. Kérem jelölje be a skálán a következő kérdések mennyire jellemzőek Önre! (1 2 3 4 5)

Ön szerint a mindennapi felhasználóknak van oka félni a hacker-ek tevékenységétől?

8. Ön szerint az utóbbi időben megnövekedett terrortámadások hatására, jobban kellene ügyelnünk az informatikai biztonsággal kapcsolatos kérdésekre?

- Igen
- Nem

9. Hallott már az Európai Unió kiberbiztonsági stratégiájáról?

- Igen, hallottam már róla, tudom, hogy mit tartalmaz.
- Hallottam már az EU-s kiberbiztonsági stratégiáról, de pontosan nem tudom mit jelent.
- Soha nem hallottam még.
- Nem tudom.
- Egyéb

10. Ön részt szokott venni internetes nyereményjátékokon?

- Igen
- Nem
- Nagyon ritkán
- Nem tudom
- Egyéb

11. Amennyiben igen, mennyire jellemző, hogy személyes adatokat ad meg a nyereményjáték miatt? (1 2 3 4 5)

12. Ön közösségi oldalakon aktív tag?

- Igen, naponta/hetente többször használom.
- Tag vagyok, de egy hónapban csak párszor jelentkezem be.
- Nem vagyok tag semmilyen közösségi oldalon.
- Nem tudom.

13. Amennyiben Ön aktív tag, milyen gyakran jelölik be ismeretlen, gyanús alakok?

(1 2 3 4 5)

14. Visszajelöl teljesen ismeretlen, gyanús személyeket közösségi oldalakon?

- Igen, miért ne jelölném?
- Nem, nem fogadom el a jelölését.
- Nem jelöltek még ismerősnek ilyen személyek.
- Nem tudom.

15. ATM-ből történő készpénzvelvételnél mindig figyelek arra, hogy ...

- Körbenézzek, nem állnak-e túl közel hozzám.
- Kezemmel eltakarjam a PIN kódom.
- Megnézzem nincs-e hamis ATM billentyűzet az automatán.
- Megfigyeljem, nem helyeztek-e fel az ATM-re bankkártya mágnescsík leolvasó készüléket.
- Egyéb

Hallgatói Nyilatkozat

Ganczer Laura, a SZIE GTK Emberi erőfrrások szakos, BSc., BKH nappali képzésben résztvevő 3. évfolyamos hallgató nyilatkozom, hogy a 2016/2017. tanévi Tudományos Diákköri Konferenciára

„Az információs biztonságvédelem tudatosságának vizsgálata a ma élő hat generáció hozzáállásának tükrében ”

címmel benyújtott pályamunka a saját munkám eredménye, a felhasznált irodalmat és adatokat korrekt módon kezeltem.

Jelen nyilatkozatommal*

- hozzájárulok ahhoz, hogy a benyújtott pályamunkám – *annak szóbeli előadását követően* – a Kari TDK Adatbázison keresztül mások számára elektronikus formában hozzáférhető legyen, valamint a Szent István Egyetem Gazdaság- és Társadalomtudományi Kar valamely intézetének könyvtárában megtekinthető (nem kölcsönözhető) legyen.
- hozzájárulok, hogy pályamunkám – *annak szóbeli előadását követően* –a Szent István Egyetem Gazdaság- és Társadalomtudományi Kar valamely intézetének könyvtárában megtekinthető (nem kölcsönözhető) legyen.
- kérem, hogy pályamunkámba csak a bírálók és a SZIE GTK TDK Szekció bizottsága tekinthessen be, mert a pályamunka adattartalma miatt pályamunkám titkosítását kértem (csak pályamunkába behelyezett titkosítási kérelem esetén választható!).

Jelen nyilatkozatommal*

- hozzájárulok ahhoz, hogy az általam beküldött fotó a SZIE GTK TDK rezümé kötetben megjelenjen.
- nem járulok hozzá, hogy a fotóm a SZIE GTK TDK rezümé kötetben megjelenjen.

*A megfelelő választ – *döntése alapján* – kérjük, aláhúzással jelölje! Valamely válasz kiválasztása kötelező!

Budapest, 2016. október 31.

……

hallgató(k) aláírása

Témavezetői Nyilatkozat

Dr. Szilágyi Tivadar, a SZIE GTK RGVI tanszékvezető egyetemi tanára nyilatkozom, hogy Ganczer Laura, a SZIE GTK Emberi erőforrások szakos, BSc., BKH nappali képzésben résztvevő 3. évfolyamos hallgató iránymutatásommal készítette a

„Az információs biztonságvédelem tudatosságának vizsgálata a ma élő hat generáció hozzáállásának tükrében ”

című tudományos diákköri pályamunkáját.

Felelősséggel kijelentem, hogy a hallgató pályamunkáját saját kutatásaira támaszkodva készítette, a szakirodalmat és a felhasznált adatokat megítélésem szerint korrekt módon kezelte.

A pályamunkát bemutatásra javaslom a 2016/2017. tanévi Kari Tudományos Diákköri Konferencián.

Budapest, 2016. október 31.

……

témavezető(k) aláírása

RESUME

SZIE GTK TDK 2016.

„AZ INFORMÁCIÓS BIZTONSÁGVÉDELEM TUDATOSSÁGÁNAK VIZSGÁLATA A MA ÉLŐ HAT GENERÁCIÓ HOZZÁÁLLÁSÁNAK TÜKRÉBEN”

Evaluation of information security and protection awareness of the living six generation

Készítette: **GANCZER LAURA**, Szent István Egyetem, Gazdaság- és Társadalomtudományi Kar, Emberi erőforrások, Nappali képzés (BA), III. évfolyam

Témavezető: Dr. Szilágyi Tivadar, Tanszékvezető egyetemi tanár, SZIE GTK RGVI Civil Biztonság- és Védelemtudományi Tanszék

Dolgozatomban szándékozom bemutatni az információs biztonság komplex értelmezését, valamint tisztázva az alapfogalmakat, ismertetem, hogy miben is tér el egymástól az információs és az informatikai biztonság területe. Célom felsorolni az ezzel kapcsolatban felmerülhető veszélyforrásokat, amelyek mindennapi gyanútlan cselekményeinket átszőhetik, és ezzel kapcsolatban törekszem a megismerésére annak, hogy a ma élő hat generáció milyen szintű tudatossággal cselekszik e veszélyek kivédésének érdekében.

Kérdőíves kutatásomban fő vezérfonal a ma élő hat generáció; a Veterán generáció, a Baby-boom, az X-esek, az Y és a Z generációk, valamint az Alpha generációk hozzáállásának vizsgálata az információs biztonság területeivel kapcsolatosan.

Kérdőívem elkészítése során a kérdéseket igyekszem átfogóan úgy megalkotni, hogy kellő információhoz jussak, mind a világhálón, mind a valós térben fellelhető információs veszélyekkel kapcsolatos hozzáállásról. Megemlíteném, hogy véleményem szerint a bankkártyás fizetések, a jelszóvédelem és az információs, informatikai védelemmel kapcsolatos oktatás, figyelemfelhívás a jövőben egyre inkább sürgető feladat elé állítja az érintetteket.

Bár az ezzel kapcsolatos intézkedések haladnak a maguk útján, addig is a mindennapi felhasználónak tudatosan kell használnia a rohamosan fejlődő technika vívmányait és lehetőségeit, mivel a tudatlanság nem lehet egyenlő a felelőtlenséggel. Amennyiben tájékozódik a laikus felhasználó a kibertérben előforduló veszélyekről, meglátásom szerint kötelessége felkészülten és megfontoltan fogadni és használni az online tartalmakat, valamint a valós térben történő ügyintézéseknél is lényeges tudatosan működnie és cselekednie.