ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

NEUMANN JÁNOS
INFORMATIKAI KAR

SZAKDOLGOZAT

OE-NIK Hallgató neve: **Szabó Árpád**

2022 Hallgató törzskönyvi száma: **T/008046/FI12904/N**

Óbudai Egyetem
Neumann János Informatikai Kar
Kiberfizikai Rendszerek Intézet

SZAKDOLGOZAT FELADATLAP

Hallgató neve: **Szabó Árpád**
Törzskönyvi száma: T/008046/FI12904/N
Neptun kódja: [redacted]

A dolgozat címe:

Social engineering és biztonság tudatosság az idősebb internethasználók körében
Social engineering and security awareness among the older internet users

Intézményi konzulens: Balázsné Dr. Kail Eszter
Külső konzulens:

Beadási határidő: 2022. május 15.

A záróvizsga tárgyai: Informatikai rendszerek üzemeltetésének biztonsága
IT hálózatbiztonság

A feladat

Modern világunkban az internetképes eszközök birtoklása folyamatosan növekszik, ezzel egyidejűleg nő az internetpenetráció a digitális bevándorlók körében is, valamint nő az internetezés gyakorisága is. Az idősebb korosztály tagjai egyre nagyobb mértékben aktív résztvevői a digitális világnak. Ezzel párhuzamosan szintén megfigyelhető, a kibertámadások számának folyamatos növekedése. Nő a social engineering technikára támaszkodó támadások száma is. A kibertérben történő támadások jelentős része manipulációs, adathalász támadás. Az internetet használó idős korosztály kevésbé foglalkozik, nem ismerik, vagy nincsenek tudatában a digitális világ veszélyeivel, információbiztonsági tudatosságuk alacsony, a támadási kísérleteket nehezen ismerik fel.
A szakdolgozat célja körüljárni, hogy az idősebb generáció mennyire van tisztában a kibertér veszélyeivel, mennyi, és milyen figyelmet fordít a biztonságos internetezésre, mennyire tudatosak, ha biztonságról van szó.
A hallgató feladata bemutatni a social engineering technikákat, a digitális bevándorlókra leginkább veszélyt jelentő támadási formákat, valamint online, támadási technikákkal illusztrált kérdőíves kutatással felmérni, hogy az idősebb korosztály mennyire tudja azonosítani a támadási technikákat, mennyire biztonságtudatosak, ha a kibertérről van szó. Megoldásokat találni, milyen módon csökkenthetőek a kockázatok, és hogyan növelhető a korcsoport biztonságtudatossága.

A dolgozatnak tartalmaznia kell:

- a social engineering támadási technikák bemutatását,
- biztonság szempontjából az emberi tényezők bemutatását,
- felmérés ismertetését,
- felmérésből levonható tapasztalatokat, megállapításokat,
- javaslatot a biztonságtudatosság kialakításának, növelésének lehetőségeire, védekezési lehetőségekre.

ÓBUDAI EGYETEM * Neumann János Informatikai Kar * 1. Budapest

.....
Dr. habil. Lovas Róbert
intézetigazgató

A szakdolgozat elévülésének határideje: **2024. május 15.**
(OE TVSz 55.§ szerint)

A dolgozatot beadásra alkalmasnak tartom:

.....
külső konzulens

.....
intézményi konzulens

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Neumann János Informatikai Kar

HALLGATÓI NYILATKOZAT

Alulírott hallgató kijelentem, hogy a szakdolgozat saját munkám eredménye, a felhasznált szakirodalmat és eszközöket azonosíthatóan közöltem. Az elkészült szakdolgozatomban található eredményeket az egyetem és a feladatot kiíró intézmény saját céljára térítés nélkül felhasználhatja.

Budapest, 2022.05.10.

Szabó Árpád

Szabó Árpád

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Neumann János Informatikai Kar

KONZULTÁCIÓS NAPLÓ

Hallgató neve: SZABÓ ÁRPÁD

Neptun Kód: [redacted]

Tagozat: KIBERBIZTONSÁGI SZAKEMBER

Telefon: [redacted]

Levelezési cím: [redacted]

Projektmunka címe magyarul:

Social engineering és biztonság tudatosság az idősebb internethasználók körében

Projektmunka címe angolul:

Social engineering and security awareness among the older internet users

Intézményi konzulens: BALÁZSNÉ DR. KAIL ESZTER

Külső konzulens: -

Alk.	Dátum	Tartalom	Aláírás
1.	2022.02.25.	A félévben teljesítendő, tervezett munka megbeszélése.	Kail
2.	2022.03.16.	Időközben felmerült problémák megbeszélése.	Kail
3.	2022.04.11.	A félévi munka véglegesítése, átbeszélése.	Kail
4.	2022.05.09.	szakdolgozat véglegesítése, prezentáció megbeszélése.	Kail

A hallgató a Projektlabor 1. / 2. / 3. / Záródolgozati projekt[1] tantárgy követelményét teljesítette, beszámolóra/védésre[2] bocsátható. A javasolt érdemjegy:

.....Kail.....

Balázsné Dr. Kail Eszter

Budapest, 2022.05.10.

---

[1] A megfelelő bekarikázandó/aláhúzandó!

[2] A megfelelő aláhúzandó!

TARTALOMJEGYZÉK

1 BEVEZETÉS

A mai modern világunkban folyamatosan növekszik az internetképes eszközök száma, és ezzel egyidejűleg nő az internetpenetráció a digitális bevándorlók körében is. Az idősebb korosztály tagjai, egyre nagyobb mértékben aktív résztvevői a digitális világunknak. Ezzel párhuzamosan megfigyelhető a kibertámadások számának folyamatos növekedése, melynek egy jelentős része manipulációs, adathalász támadás, melyek az úgynevezett social engineering technikákra támaszkodó támadások, melyekkel ezen idősebb korcsoport tagjai a leggyakrabban találkozhatnak, és teheti próbára esetleges biztonságtudatosságukat. Annak érdekében, hogy pontosabb képet is kapjunk, megállapítható, hogy a kibertérben elkövetett támadások 98%-a social engineering módszereken alapul. [1] A Központi Statisztikai Hivatal 2022. január 05. napján, a 2021. III. negyedévre vonatkozó jelentése megállapítja, hogy a digitalizáció, az internethasználat – a járványhelyzetből is adódóan – számottevő módon a mindennapok részévé vált. „A helyhez kötött (vezetékes és helyhez kötött vezeték nélküli) internet-előfizetések száma 2021. III. negyedév végén 3,3 millió volt, 2,3%-kal több az egy évvel korábbinál.” [2] Továbbá a Statisztikai Hivatal közreadott számai szerint Magyarországon az internethasználók aránya (16–74 éves népesség százalékában) a 2017. évi 77%-ról, a 2020-as évben 85%-ra nőtt, és ez a szám, ha már kismértékben is, de folyamatosan növekszik. [3] Ezen statisztikai jelentések alapján is könnyen következtethetünk a digitális térben, az idős korosztályt váró veszélyekre.

Az idősebb korosztály alatt szakdolgozatomban az úgynevezett „baby boom” korszak generációját értem, akik 1946 és 1965 között születtek, és akik már csak felnőttkorukban találkoztak, ismerkedtek meg az informatikával, digitális világgal, infrastruktúrával, és az ezt jellemző infokommunikációs, digitális eszközökkel, ezért jellemzően nehezen tudnak, tudtak alkalmazkodni ezen információtechnológiai fejlődéshez. Nehezebben felelnek meg a már mindennapokat jellemző digitális kihívásoknak is. Ezen generáció tagjai, vagy már nyugdíjas éveiket töltik, vagy éppenséggel még aktív keresők. [4] [5]

Rövid személyes példával szeretnék rávilágítani, mi a célom a szakdolgozattal, miért ezt a témát választottam, és mit kívánok majd bemutatni.

Budapesti bankfiókban várakoztam, várva a soromra, egy olyan üggyel kapcsolatban, melyet csak személyesen tudtam elintézni. Előttem egy láthatóan nyugdíjas korú hölgy próbálta elintézni banki dolgait, azonban ez nehézséget okozott, tekintettel, hogy hallókészüléket viselt és nehezen értette az ügyintézőt, aki így szinte kiabált, és ezen még a maszkviselés sem segített. Ez számomra egy érdekes helyzetet teremtett, talán jellemezhetem, hogy egy önkéntelen, kifordított, bár nem a fogalom legszorosabb értelmében vett social engineering történt, ugyanis az ügyintézés alatt megtudtam az utánam várakozókkal együtt az ügyfél ott beállított Telebankos jelszavát, - amire megjegyezte, hogy ezt könnyen észben tudja tartani, tehát valószínűleg más szolgáltatásnál is használja ezt a jelszót – valamint az ehhez kapcsolódó négy számjegyből álló, rögzített internetes vásárlási jelszavát. Érthetetlen okból ezt nem

írásban kommunikálták le. Ez a helyzet elgondolkodtatott, vajon az ügyfél mennyire volt tisztában a cselekmény veszélyével, a hozzá hasonló időskorúak, akik nem régóta, vagy csak most csatlakoztak fel a világhálóra, mennyire vannak tisztában a kibertér veszélyeivel, mennyi, és milyen figyelmet fordítanak a biztonságos internetezésre, mennyire tudatosak, ha biztonságról van szó, ismerik, felismerik-e a leggyakrabban jelentkező social engineering támadásokat, technikákat. Mennyire érintheti őket, mennyire vannak felkészülve az ilyen jellegű támadásokra.
Hiszen ma már aki használja a világháló adta kényelmet, nagy valószínűséggel ott intézi személyes ügyeit is, kezdve az elektronikus levelezésen, online vásárláson keresztül a különböző (banki, közüzemi) szolgáltatások igénybevételéig. A jelenlegi járványhelyzet talán fel is gyorsította ezen időskorú generáció digitális világba történő becsatlakozását, és egyre több irányba történő felhasználását, és talán ez okból kifolyólag, szervesebb része lett hétköznapjaiknak is.
Szakdolgozatomban a fent felvetett kérdésekre keresem a válaszokat, melynek első felében próbálom megfogalmazni, mit is jelent pontosan, majd bemutatni a „baby boom" generációra leginkább veszélyt jelentő social engineering támadást, az ezt jellemző technikákat. Ezen támadási technika jellemzően valamiféle pszichológiai manipulációt jelent, melynek középpontjában az ember helyezkedik el, így egy fejezetben megvizsgálom, milyen emberi tényezők játszhatnak szerepet sikerességükben, mik azok az emberi tulajdonságok, amik a sikeres támadás egyik kulcsát, elemét adja, adhatja.
Dolgozatom második felében online kérdőíves felmérést készítettem, az időskorú generáció körében, melynek segítségével próbálok a felmerült kérdésekre válaszokat találni, információbiztonság tudatosságukat felmérni, illetőleg ebből következtetéseket levonni. A kérdőív két részből áll, az első rész az általános demográfiai kérdéseken túl, a számítógép, és ehhez kapcsolódóan az internethasználati kérdésekből tevődik össze. Ezt követi a kérdőív második fele, ahol 12 bemutatott e-mail üzenet legitimitását kellett megítélni a válaszadónak, vagyis mely üzenet lehet valódi, illetőleg nem valódi, jellemzően adathalász levél, röviden indokolva a választás okát is. [5] [6] [7] [8]

Kutatásom hipotézisei a következők:

1. Ezen korosztály nem használ biztonsági programokat, nem ismeri, nincs felkészülve a veszélyekre, de találkoztak már social engineering támadással, adathalász levelekkel.
2. Azon személyek, akik nem változtatták meg alapbeállított Wifi jelszavukat, eszközeiket sem védik meg biztonsági szoftverekkel.
3. Ezen korosztály a jelszavakat papírra írva tárolja otthon, és ha tehetik a lehető legegyszerűbb karakterkombinációjú jelszót használják.
4. Azon személyek, akik bonyolult, nehezen megjegyezhető jelszót használnak, több helyen is használják ugyanazt a jelszót.

Fontos megfogalmaznom, mit is értek a címben szereplő biztonságtudatosságon. Maqousi és szerzőtársai alapján: „Az információbiztonsági tudatosság egy olyan folyamatos tanulási folyamat, melynek értelme van a fogadó fél számára és mérhető hasznot hajt a szervezetnek a tartós viselkedésváltozáson keresztül." ("Information security awareness is an ongoing process of learning that is meaningful to recipients and delivers measurable benefits to the organization from lasting behavioural change.") A megfogalmazott koncepción értem azt is, amikor az egyénnek is hasznot hajt az információbiztonsági tudatosság, és amely elsősorban az informatikai tárgyú esetekre korlátozódik. [9] [10]
Más megfogalmazásban, amikor információbiztonsági tudatosságról, "security awareness"-ről beszélünk, akkor a megszerzett, vagy oktatott tudás alkalmazását értem alatta. [11]

Dolgozatom végén megpróbálok megoldásokat keresni, javaslatokat megfogalmazni, hogy a kérdéses korosztályt a kibertérben fenyegető veszélyektől hogyan, milyen módon lehet megvédeni, milyen eszközökkel lehet kivédeni, megelőzni a támadásokat, csökkenteni a kockázatokat, vagy az esetlegesen bekövetkezett támadás esetén minimalizálni a károkat, illetőleg növelni biztonságtudatosságukat.

2 SOCIAL ENGINEERING FOGALMÁNAK MEGHATÁROZÁSA

Kulcsfontosságú értelmezni, és tisztázni e fogalmat, majd ebből kiindulva meghatározni a típusait. Hisz így megérthetjük, pontosabb képet kaphatunk, milyen elvek mentén, milyen technikákkal dolgozik, és végső soron miért az egyik leghatásosabb, és az egyik legnagyobb veszélyt jelentő támadási forma a háború után született generációra nézve is, valamint esetlegesen miért áshatja alá a vélt, vagy valós biztonságba vetett hitüket.

Kevin D. Mitnick a műfaj valaha legnagyobb művelőjének a megfogalmazásában „a social engineering a befolyásolás és rábeszélés eszközével megtéveszti az embereket, manipulálja vagy meggyőzi őket, hogy a social engineer tényleg az, akinek mondja magát. Ennek eredményeként a social engineer – technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni.” [12]
Tulajdonképpen egy olyan támadási típusról beszélhetünk, ami az emberi psziché kihasználható jellemvonásain, sajátosságain alapul, olyan eljárásmódok, mind technikai mind egyéb módszerek összessége, amely az emberek kihasználásával, befolyásolásával szerzi meg a szükséges információkat, az adott rendszerhez a hozzáférést, esetlegesen a kártékony programok terjesztését. [13] [14]
Ezen módszerek segítségével az emberi pszichológia, befolyásolhatóság kiaknázása révén, adatokhoz, számítógépes rendszerekhez, információkhoz juthatunk. [15] Ebből kifolyólag social engineering támadások kockázatát az emberi tényező adja, mivel az ember, a célszemély az aki rendelkezhet a támadó számára szükséges információval, hozzáféréssel, és lássuk be, megtéveszteni is a legkisebb erőfeszítésbe kerül. [16]
Ebben a rendszerben az embereket tekintjük a leggyengébb láncszemnek, gyakorlatilag itt nem a technikai biztonság, hanem az emberi biztonság problémája áll fenn, így a meggyőzés, manipuláció, megtévesztés technikájával a jogosulatlan személy privát információkhoz juthat, vagy olyan cselekedet, művelet végrehajtására ösztökélhet, ami végső soron nem áll a jogosult érdekében. [17]
A social engineering támadások révén a kiberbiztonsági rendszerek is kikerülhetőek, kihasználva, manipulálva az embert mint a biztonság leggyengébb láncszemét, akik nem is lesznek tisztában cselekedeteik rombolásával, a biztonsági eljárások megsértésével, vagy egyáltalán azzal, hogy manipulálták. Mindazonáltal a támadó, technikai eszközöket is bevethet céljának leghatékonyabb elérése érdekében. Ezekre a támadásokra az embereket fel kell készíteni, ki kell képezni, mert legtöbbször nem lehet megakadályozni szoftveres vagy hardveres megoldásokkal, és az esetek többségében a támadó nem kerül szembe az áldozattal. [18] [19] [20]
Más megfogalmazásban a social engineering a művészete, vagy még inkább tudománya minden olyan cselekménynek, ami szándékosan befolyásolja az embert annak érdekében, hogy a céljainkat elérjük. [21] [22]
Ez alapján a social engineering technikák célja nem a számítógépes rendszer lesz, hanem az emberi természet, azonban e technikák nagymértékben különbözhetnek, nem csak pszichológiai trükkökre korlátozódhat, hanem a támadók ugyanúgy használhatnak

különböző kellékeket, vagy akár még álruhákat is, és alkalmazhatóak más platformokon is, például telefonhívás, e-mail, vagy weboldal. [23]

A fogalom gyakorlatiasabb megértése érdekében, dolgozatom következő szakaszain a különböző támadási technikák bemutatására vállalkozom.

3 SOCIAL ENGINEERING TÁMADÁSI TECHNIKÁK BEMUTATÁSA

Kevin D. Mitnick definíciójában láthattuk a social engineer használatához nem feltétlenül szükséges technológia tudás, nemcsak azok használatával érhetjük el célunkat, így ez alapján, két fő kategóriába sorolhatjuk a támadásokat. Beszélhetünk az emberi tényezőt jobban kihasználó humán alapú, és a számítástechnikai tudáson alapuló támadásokról, illetőleg akár vegyesen is használhatóak e technikák, az elérendő cél függvényében. Így előfordulhat, hogy a különböző módszerek egymásra építése hozza meg a sikert. A technikai tudáson alapuló támadás középpontjában a félrevezetés áll, ilyenkor a támadó elhiteti a felhasználóval, hogy egy „igazi" alkalmazással vagy rendszerrel lép kapcsolatba, és a bizalmas információk megadására készteti. Ilyen lehet például amikor egy az eredetivel szinte megegyező álweboldalon újra hitelesítési információk (felhasználónév, jelszó) megadására késztetnek. Így a támadó hozzáférhet a megadott azonosító adatunkhoz. A nem technikai tudáson alapuló támadások középpontjában az emberi gyengeségek kihasználása áll, mely során a támadó közvetlen interakcióba is kerül a célponttal, ilyen lehet például egy áltelefonhívás, amikor a támadó magas rangú vezetőnek adja ki magát. [7] [20] [24]

Fontosnak tartom megemlíteni, hogy a social engineering támadások, ideértve mind a technikai mind a humán alapút, különböző csatornákon mennek végbe, amin keresztül a támadó végrehajtja támadását. A csatornák leggyakrabban az alábbiak lehetnek: mobil-, azonnali üzenetküldő alkalmazások, e-mail, közösségi média felületek, telefon, közvetlen fizikai találkozás, interakció, felhőszolgáltatások, webhelyek, weboldalak. [23]

3.1 Humán alapú technikák

Segítség kérése: Mint ahogy a neve is mutatja az egyik legkönnyebben kivitelezhető támadási forma, megtervezése sem jelent bonyodalmat, egyszerűen segítséget kérünk egy munkatárstól, kihasználva segítőkészségét, jóhiszeműségét, és így jutunk hozzá a szükséges információhoz. Ilyen támadás lehet például amikor egy új munkatársnak adjuk ki magunkat, és ezt kihasználva kérünk segítséget. Így akár a megszerzett információval előkészítve, megalapozva egy következő támadást. Ilyen jellegű támadás érheti még a HelpDesk-en, titkárságon, ügyfélszolgálaton, vagy recepción dolgozókat is, mert ők azok, akik legtöbbször rutin munkát végeznek, emberekkel foglalkoznak, sokszor hasonló megkeresésekkel nap mint nap, így nehezebben is szűrik ki a valótlan megkereséseket. [4] [13]

Segítség nyújtása: Melyet fordított social engineernek is neveznek, ilyenkor általában a támadó okozza a problémát, és úgy alakítja a helyzetet, hogy a célszemély hozzá forduljon segítségért, és ő lesz az, aki tudásával megoldja, elhárítja a problémát, hogy hálánkat kifejezve, mi is segítsünk neki, így szerezve meg a szükséges információkat. Ez

a típusú támadás információtechnológiai megoldásokkal együtt is jól tud működni, a kölcsönösség kihasználásával, ilyen például, amikor egy hamis weboldalon kínálnak valamilyen ingyenes vonzó tartalmat, regisztrációért cserébe, a felhasználó megadja e-mail címét, jelszavát, és amennyiben máshol is használja a megadott adatokat, a támadók máris megszerezték a hozzáférést. [4]

Megszemélyesítés: Identitáslopásnak is nevezik, vagyis amikor gyakorlatilag hamis személyazonosságot vesz fel a támadó, másik személynek adja ki magát, ami szinte az összes humán alapú támadást is jellemzi. Többféle típusa van, kiadhatja magát a támadó, – és így álruhába is bújhat – karbantartónak, rendszergazdának, takarítónak, futárnak, ezeket az embereket a munkavállalók általában kevésbé ismerik. Álcázhatja magát másik alkalmazottnak, fontos embernek, például egy másik osztály vezetőjének, külsős munkatársnak, vagy akár egy elhunyt dolgozó identitását is használhatja, akinek az adatai még nem törlődtek a rendszerből, és ilyen módon tévesztve meg a dolgozókat, megszerezve az információkat, adatokat. [4]

Shoulder surfing – „váll szörfözés": E módszer során is felvehet hamis személyazonosságot a támadó, elég ha közel kerül a célszemélyhez, ehhez például kiadja magát informatikai munkatársnak, és valamilyen hamis ürüggyel megkéri a munkavállalót lépjen ki, majd be, az egyik rendszerbe, és ilyenkor kilesi a belépéshez szükséges adatokat. [4]

Tailgating: Épületbe bejutás technikája, amikor a támadó egy csoporttal jut be az épületbe hozzájuk csapódva, kihasználva az őrök figyelmetlenségét. Nagyobb előkészületet igényel, ilyenkor valamilyen álcát is felvesz a támadó, ilyen lehet például amikor egy takarító brigádhoz csatlakozva jut be az épületbe. [4] [14]

Piggybacking: Épületbe bejutás másik technikája, amikor a támadó más jogosultságát hamisan használja fel, például valamelyik munkatásnak kiadva magát, aki véletlenül otthon hagyta a belépőkártyáját, és ezt kihasználva juthat be az épületbe, az őrök segítségével. [14]

Dumpster diving – kukabúvárkodás: Ez esetben a kiválasztott célszemély szemetesét túrja át a támadó, felhasználható információkhoz, adatokhoz jutás reményében, szintén lehet egy másik támadás megalapozása, előkészítése. [1] [14]

Jelszavak kitalálása: Itt nem informatikai technikát használva, szoftver segítségével törjük fel a jelszavakat, hanem a jelszóhasználati szokásokat, a gyenge jelszavak megválasztását használja ki a támadó. Amikor túl egyszerű, vagy a személyünkre utaló jelszót választunk, vagy bonyolult jelszót, amit feljegyzünk valahova. E technika előzménye lehet például amikor a kukabúvárkodás útján szerzünk meg információkat, vagy valamely épületbe bejutás technikája során, és így egymásra építve, kihasználva a humán alapú támadásokat. De ebből a szempontból nézve, a támadók kihasználhatják a közösségi oldalakon magunkról közzé tett személyes információkat is. Meglepő módon

azonban sokszor a jelszavak kitalálásánál nem szükséges a személy alaposabb ismerete sem, mint ahogy az láthatjuk a 3-1. ábra és 3-2. ábra alapján, ahol rangsorrendben szerepelnek a leggyakrabban használt jelszavak. [1] [4]

3-1. ábra: A 30 világszerte leggyakrabban használt jelszó [25]

3-2. ábra: A 10 leggyakrabban használt magyar jelszó [26]

Elengedhetetlennek tartottam bemutatni a humán alapú támadási technikákat is, még ha a felsorolás közel sem teljes, és részletes. Azonban úgy gondolom az ilyen típusú támadások a módszerből adódóan a nagy szervezeteknél hatékonyak, és ott is fordulhatnak elő a leggyakrabban. Véleményem szerint a szakdolgozatom fókuszában lévő időskorú digitális bevándorlók ritkán találkoznak e támadási formákkal, még az esetben is, ha aktív munkavállalók.

IT alapú módszerrel végrehajtott technikával való találkozás, már csak a kivitelezés módja miatt is, sokkal gyakoribb lehet. Fontos jellemzője, hogy személyes kontaktus nem történik, így számítógépen, tableten, vagy okostelefonon keresztül megy végbe a támadás, kihasználva az emberi hiszékenységet. Az áldozat nem is veszi észre, hogy csalás áldozatává vált, hogy a „hamis" rendszerrel lépett kapcsolatba. [1] [7] A leggyakrabban az időskorúak ezzel a technikával találkozhatnak, ez jelenti rájuk a legnagyobb veszélyt, az otthoni, vagy akár munkahelyen történő internetezés közben.

3.2 Számítógép alapú technikák

Adathalászat: Leggyakoribb, legelterjedtebb technikákat foglalja magába, nagyon sok válfaja létezik, attól függően, hogy a social engineerek milyen csatornán hajtják végre a támadásokat. A legjellemzőbb valamilyen elektronikus csatornán, például e-mailben végrehajtott támadások. Döntő többsége tömeges támadásnak minősül, tömegeket megcélzó, nagy célcsoporttal, hogy a lehető legtöbb áldozatot elérjék, ilyen esetben nem személyre szabott az üzenet, a támadásnak nincs a címzetthez igazított része. Azonban célzott támadás formájában is használják, kiválasztva például egy adott szervezeten belül egy felsővezetőt, előzetesen információt gyűjtve róla. Ebben az esetben az üzenet bizonyos mértékig az áldozatra szabott. A cél minden esetben különböző információk (általában jelszavak, e-mail címek, hitelkártya adatok, banki adatok) megszerzése, valamely kiválasztott elektronikus csatorna segítségével. [1] [18] [27] [28] [29]

3-3. ábra: Adathalász e-mail, a szerző saját e-mail fiókjából

Phishing: Az adathalászat angol kifejezése, mely az esetek döntő többségében az e-mail az egyik leggyakoribb csatornája. Ilyenkor általában az üzenetben elhelyezett linken keresztül egy hamis weboldalra irányítják a gyanútlan áldozatot, ahol bizalmas adatok megadására kérik, mint ahogy láthatjuk is kiemelve a linket a 3-3. ábra adathalász email üzenetén. Jellemzője egy állevél valamelyik banktól, vagy szolgáltatótól, amiben

valamilyen információ ellenőrzést kérnek sürgetve, és figyelmeztetve a súlyos következményekre, ha nem tesszük meg. Az üzenet tartalmazza a csaló weboldalra mutató linket, mely a céges logók és tartalom alapján kísértetiesen hasonlít az eredetihez, és olyan űrlappal rendelkezik, amely felhasználónév, jelszó, kártyaszám vagy egyéb adatok megadását kéri. Manapság már a legtöbb weboldal https biztonságos protokollt használ, ugyanis itt egy tanúsítvány igazolja, hogy a weboldal tényleg az akinek mondja magát, ilyenkor a címsorban egy lakat szimbólum szerepel. Azonban ez még nem jelenti, hogy az oldal tényleg biztonságos, vagy megbízható, ugyanis a csalók ingyenes tanúsítványukat biztosító cégektől szerzik meg a hamis a weboldalhoz szükséges tanúsítványukat, melyek csak a címsorban szereplő hivatkozás eredetiségét igazolják, azt nem, hogy a weboldal mögött álló cég, szervezet, vagy magánszemély kicsoda. Ez nagy figyelmet kíván a felhasználótól, mert a legtöbben a címsorban szereplő lakat láttán megnyugszanak, pedig mindenesetben rá kell kattintani a lakatra, mert ott találhatók a részletes információk melyből kiderülhet, hogy igazából egy csaló weboldallal állunk-e szemben. Ez különösen fontos olyan weboldalaknál, például banki szolgáltatást nyújtó oldalak, ahol különösen érzékeny információk megadását kérik. Előfordulhat, hogy a levél linket nem tartalmaz azonban a formája, mind logókkal együtt megegyezik az eredeti céges levéllel, így nagyon nehéz megkülönböztetni az eredetitől, ilyenkor árulkodó lehet az e-mail cím formája. Ez esetben általában a súlyos következményekre szintén figyelmeztetve a levélben magadott bankszámlára kérnek utalást, például az elmaradt díjbefizetéssel kapcsolatban, valamely közszolgáltató nevében, meghamisítva eredeti levelüket. Ahogy a 3-4. ábra egy hamisított banki adathalász e-mailt mutat be, az eredetihez megtévesztésig hasonló logókkal. Hitelesség érdekében ezek az e-mailek tartalmazhatnak, felhasználónevet, személyes adatokat is. Az adathalász e-mailek egy jelentős részére jellemző, hogy rosszul kidolgozottak, az üzenetek nyelvtani hibákat, vagy helytelenül írt szavakat tartalmaznak, vagy magyartalan mondatokat, amennyiben valamilyen internetes fordítóprogram segítségével fordították le a szöveget.

Amennyiben adathalász támadással a csaló hozzáférést szerez az e-mail fiókunkhoz, a legnagyobb problémát az fogja jelenti, hogy így hozzáférést tud szerezni minden olyan online szolgáltatás felett is, amely az adott fiókunkhoz kötődik. [1] [14] [20] [27] [28] [29] [30] [31]


OB

OTP Bank
info@otpdirekt.hu
Részletek elrejtése

Dátum: 2019. aug. 6. 11:37

Fontos tájékoztató a OTPBank szolgáltatással kapcsolatban

Tisztelt Ügyfelünk!

Ezúton szeretnénk tájékoztatni, hogy az EU 2015/2366 irányelv (PSD2) erös ügyfél- hitelesítésröl szóló rendelkezéseinek biztositása érdekében 2019. August 15-től megszünik a OTPdirekt Internet Service szolgáltatásba, hogy megbízható ügyfél-hitelesítési rendelkezéseket biztosítson az EU 2015/2366 (PSD2) irányelvben. Kérjük, frissítse az OTPdirect szolgáltatását 2019. augusztus 15-ig.

https://www.otpbank.hu/internet-banking/OTP2871

Üdvözlettel,
OTP Bank Nyrt.

otpbank

3-4. ábra: Adathalász e-mail [32]

Spear phishing: célzott adathalászatnak nevezik, az olyan döntő többségében elektronikus levéltámadási technikát, amikor a célszemélytől előzetesen információt gyűjtenek, így a levél szövege sokkal hihetőbbé válik. Ezért az ilyen jellegű technikai támadás estén sokkal valószínűbb a támadás sikeressége, tekintettel, hogy az üzenet személyes információkat is tartalmaz. Amellett, hogy a levél a címzettre jellemző információkat tartalmaz, a szerkesztettsége, szövege is jobban kimunkált, nem tartalmaz elírásokat, nyelvtani hibákat. Ez a támadás nagy erőfeszítést és kutatómunkát igényel, ezért általában ismert személyek, vállalati vezetők a célszemélyek, de előfordulhat, hogy magánembereket támadnak meg, ilyenkor már a név, cím, telefonszám alapján jól célzott hamis e-mail üzenetet küldhetnek például fiktív számlatartozással. Tekintve, hogy ilyenkor a levél személyesebb, így jobban bízunk benne, könnyebben válunk csalás áldozatává. [29] [31]

Röviden kitérve, itt kívánom bemutatni, hogy a célzott, akár egyetlen felhasználót megcélzó social engineering támadások során, mind a humán, ahol interakcióba kerülhet a támadó és a célpont, mind az IT technikai alapú támadás – utóbbira az egyik legjobb példa az előbb bemutatott spear phising – minden esetben egyfajta egységes mintát mutat, mely alapján különböző szakaszokra, lépésekre bontható.

Az első szakasz, amely alapot teremt a következő lépéseknek, a kutatás fázisa, ahol támadók kiválasztják a célszemélyt, majd információkat gyűjtenek róla. Az információk származhatnak különböző online, offline forrásokból, például közösségi oldalak, nyilvánosan elérhető dokumentumok, cég honlap, vagy akár kellően előkészített többlépcsős támadás kivitelezése esetén, humán alapú támadásból is. A következő lépés a kapcsolat kialakítása, kiépítése, az összegyűjtött információkat felhasználva, hogy a

célszemély bizalmába férkőzhessenek, mely történhet közvetlen kapcsolatfelvétel, vagy e-mail kommunikáció útján is. Majd a kapcsolat kihasználása, kiaknázása következik, vagyis a támadás végrehajtása, a kívánt információk megszerzésére. Végezetül ezt követi a befejezés szakasza, ami a támadás befejezését jelenti, amikor a támadó nyom nélkül „kisétál, kilép a támadás helyszínéről". [14] [19] [29] [33]

Kéretlen e-mail (spam): Másik típusa az adathalász e-maileknek amikor a csatolmányaiban különböző típusú kémprogramokat, hátsó ajtókat, zsarolóvírusokat rejtenek el, és gyanútlanul megnyitva a csatolmányt, azok aktiválódnak az áldozat gépén. Előfordul, hogy a támadók gyakran az üzenettel együtt párosítják a rosszindulatú programokat is, így már csupán csak megnyitva az e-mailt, települhet a program, amely szintén szerezhet információkat a felhasználóról. Sok esetben a kártékony kódokat tartalmazó üzenetek úgynevezett spam levélként érkeznek elektronikus postaládánkban, melyek irrelevánsak, kéretlenek, és nagy tömegben érkeznek, és melyben különböző trükkökkel manipulálnak a támadók az elhelyezett csatolmány megnyitására, kihasználva kíváncsiságunkat, figyelmetlenségünket. Ilyenkor általában valamilyen hasznosnak vélt információval csapnak be, amelyek például lehetnek ajándékokra, ingyenes vásárlási kuponokra, különféle ingyenes képekre, zenékre, videókra, szórakoztató tartalmakra, ingyenes szórakozási lehetőségekre, ingyenes szoftverletöltésre való felhívás is. Abban az esetben, ha sikeresen feltörték valamelyik barátunk, ismerősünk, vagy rokonunk e-mail címét, akkor akár onnan is kaphatunk kártékony programot tartalmazó levelet, mely így még a gyanúnkat sem kelti fel. [1] [14] [15] [20] [27] [28] [30]

Ál weboldal: Klasszikus formája amikor egy hamis weboldal, regisztrációért cserébe nyereményeket ígér, így megszerezve az e-mail címeket, felépítve egy adatbázist, felhasználva egy későbbi adathalász támadáshoz. Figyelemfelkeltő, kattintásvadász linkkel is átirányíthatnak a támadók olyan weboldalra, ami fertőzött, de e-mailben is megjelenhet akár egy kattintásvadász hirdetés, vagy reklám, ami fertőzött oldalra irányíthatja az áldozatot. [1] [14]

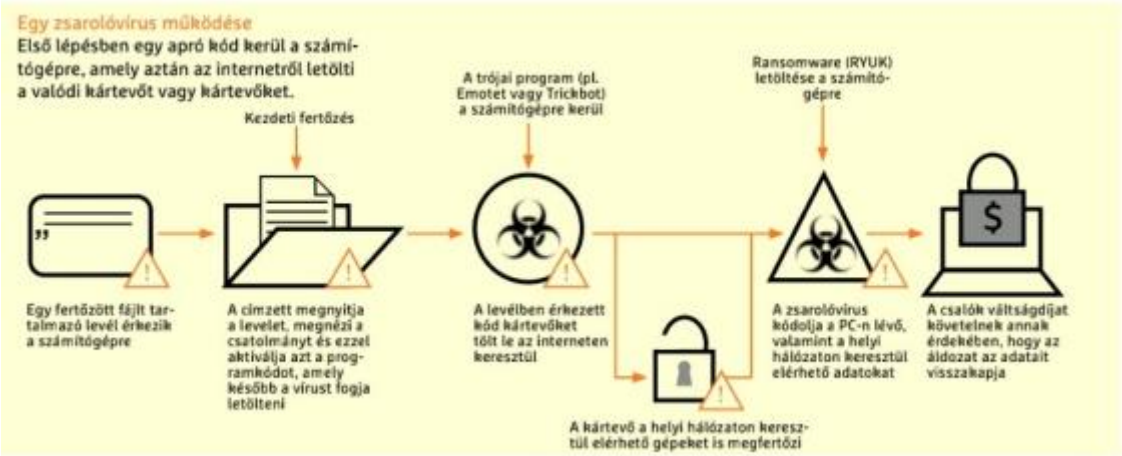
Typosquatting: A typosquatting olyan hibákra utal, amikor a felhasználók az internetes címek gépelése során apró hibákat követnek el, és véletlenül rosszul írják a felkeresni szándékozott weboldal címét. Az adathalászatnak azon formája amely során a kiberbűnözők ismert weboldalak alapján szándékosan rosszul írt neveket tartalmazó domaineket regisztrálnak. Így a látogatók olyan alternatív webhelyekre juthatnak, amelyek ugyan hasonlíthatnak az eredetire de abban a reményben, hogy azon felhasználók, akik ezt nem veszik észre, ezen alternatív weboldalakon személyes adatokat, felhasználónevüket, jelszavukat, vagy például hitelkártya- vagy banki adatokat adnak meg. Ez a támadási forma kiemelten támaszkodik az egyszerű emberi hibákra, félreértésekre. Gyakori, hogy a felhasználó nem gépelési hibát ejt, hanem egész egyszerűen nincs tisztában a weboldal címének helyes írásmódjával.
„A typosquatting egy változata az úgynevezett combosquatting. Ilyenkor a bűnözők olyan domaineket regisztrálnak, amelyek némileg eltérnek a törvényes domainektől, és további

szavakat adnak hozzá, például amazon-onlineshop.com, hogy a felhasználók azt higgyék, hogy ez egy törvényes Amazon weboldal. Ebben az esetben nem gépelési hibákról van szó, csupán a felhasználók megtévesztésére szolgáló további szavakról.” [34]

Watering hole: A technikához jelentős műszaki ismeretekkel kell rendelkezni. A támadást megelőzi egy kutatás amikor a támadók azonosítanak egy, vagy akár több törvényes weboldalt, amelyet a célszemély(ek) rendszeresen felkeres(nek). Majd ezek után az oldalon sebezhetőség után kutatnak, vagy feltörik a weboldalt és kártékony kódokat helyeznek el a rajta, és ezeken keresztül, vagy a talált sérülékenységeket, biztonsági réseket kihasználva – miután a felhasználó újra meglátogatta a honlapot –tudják esetlegesen az áldozat gépét megfertőzni, vagy információkat, adatokat ellopni tőle. Mivel az áldozat rendszerese felkeresi az adott weboldalt, bízik benne és nem is gondolja, hogy onnan érheti támadás. [21] [30] [35]

Kártékony programok: Egy jellemző és jelentősen nagy csoportja a számítógépes technikát igénylő támadásoknak, melyet már részben érintettünk is. Ilyen estekben rosszindulatú kódok segítségével szerzik meg a támadók a felhasználók adatait, juthatnak bizalmas információhoz, ezáltal zsarolhatják is őket. Szélsőséges esetben távoli elérést is szerezhetnek a támadók a felhasználó gépén. A legtöbb esetben a rosszindulatú programok általában a felhasználó tudta és engedélye nélkül fertőzi meg eszközeit. Típusai között találjuk az álvírusírtókat, amikor például egy felugró ablakban elhitetik a gyanútlan felhasználóval, hogy megfertőződött a számítógépe, vagy akár okostelefonja, és a támadó által felajánlott vírusírtó, esetleg frissítés fog segíteni a problémán, ezzel szemben azonban megfertőzik a kliens eszközét. Másik gyakori módszer, amikor nem ellenőrzött letöltő oldalakon keresztül tölt le a felhasználó a számára hasznos, legtöbbször ingyenes programot, és ennek letöltésével települ fel a kártékony program, mely akár trójai program is lehet. Ezek a kártevők hátsó ajtót nyitnak a megfertőződött eszközön és ezt kihasználva kémkednek az áldozat után megszerezve annak fontos adatait.
Az úgynevezett *Keylogger program* is alkalmas a bizalmas adatok megszerzésére, ilyen estben a kliens eszközön minden egyes billentyűleütést naplóz a program, melyet elküld a támadók részére. Előfordul, hogy a csalók a nagy website-okon bannereket úgynevezett digitális reklámcsíkokat helyeznek el, azonban ezekre kattintva, nem egy másik weboldalra jutunk, hanem egy rosszindulatú program, vírusos fájl töltődik le a felhasználó gépére, mely segítségével szintén hozzáférhetnek adatainkhoz.
A rosszindulati programok egy speciális fajtája a zsarolóvírusok, úgynevezett ransomware-k, melyek nagy szakértelmet kívánnak. Ezek működését mutatja be a 3-5. ábra. Céljuk a pénzszerzés a felhasználótól. Ezek a rosszindulatú programok leggyakrabban e-mail csatolmányként, vagy e-mailben egy link formájában kerül fel a célszemély gépére. A vírus a háttérben a kliens gépét, vagy az összes fájlt zárolja, titkosítja, és a feloldásért cserébe pénzt kérnek az áldozattól. Ugyanis a visszafejtéshez szükséges kódot csak a támadó által meghatározott váltságdíj kifizetése után kapja meg az áldozat, elvileg, mert semmi nem garantálja, hogy ez így is fog történni. Ezért a legjobb

védekezés ez ellen, ha már meg is történt a baj, hogy mindig készítünk biztonsági mentéseket, így az adatokat könnyedén visszaállíthatjuk, feltéve, ha a biztonsági mentést a gépünktől külön tároljuk, például külső merevlemezen. A legújabb változatok nem csak titkosítják, hanem el is lopják az adatokat a célszemély gépéről, így a támadó nagyobb sikerrel járhat, könnyebbé válik az áldozattól pénzt kizsarolni. E fajta támadás ellen a biztonsági másolat készítésével sem tudunk védekezni, és sajnos itt sincs garancia arra, hogy a kifizetés után visszakapjuk az adatainkat, vagy nem kerül fel a világhálóra. [1] [14] [27] [30] [31]



3-5. ábra: Egy zsarolóvírus működése [31]

WiFi támadás: A támadók kihasználhatják az otthoni WiFi hálózatunk gyengeségeit is, melyen keresztül megfigyelhetnek, hozzáférhetnek fontos információkhoz, vagy akár telepíthetnek rosszindulatú szoftvereket is. A legtöbb felhasználó alapértelmezetten hagyja routerének jelszavát, vagy gyenge jelszót használva, könnyű támadási felületet biztosít a támadóknak. Könnyű célpontnak számítunk az ingyenes WiFit biztosító helyeken is, mint például, szálloda, reptér, kávézó, ahol könnyen feltörhetik a hálózatot és ezt használó eszközeinket. [1] [14] [27]

Napjainkban a mobiltechnika fejlődésével, az internetet már okostelefonról, tabletről, is könnyedén elérhető, állandóan online lehetünk, és instant üzenetküldő szolgáltatásokat használunk. Ez a kényelem azonban jelentős kockázatokkal is jár, melyet a kiberbűnözők kíméletlenül kihasználnak, ha nem kellőképpen figyelünk használatára. [1]
Kártékony mobilalkalmazás: Fontos támadási felület annak ellenére, hogy nagyfokú technikai tudást feltételez, de mivel ma már mindenki zsebében ott lapulnak az okostelefonok, így ezekről is rengeteg személyes információ, adat nyerhető ki. A támadó létrehozza a káros kódot tartalmazó alkalmazást, például egy játékot, és azt feltölti az ilyen alkalmazásokat kínáló webes platformra. Majd a felhasználó által a telefonra gyanútlanul feltelepített káros alkalmazás megfertőzi a felhasználó telefonját, így a hitelesítő adatokat elküldheti a támadónak, de akár hozzáférhetnek üzenetekhez, kamera és mikrofon vezérléséhez, megosztott tartalmakhoz, geolokációs adatokhoz is. [1] [14]

Ehhez kapcsolódóan a különböző internetre kötött okos eszközök is jelentős veszélyt rejtenek magukban. Például internetre kötött otthoni kamerához is könnyedén hozzáférhetnek a megfelelő tudással rendelkező támadók, így nemcsak egyszerűen a privát adatokat szerezhetik meg, de behatolnak a legszemélyesebb privát szféránkba is.

Smishing: Csaló sms-ek, amikor az sms-t használja ki a támadó, hogy az üzenetben lévő linket megnyissa az áldozat, mellyel káros program települ mobileszközére, vagy hamis weboldalra irányít, de jellemző az is amikor különböző ürügyekkel (pl.: koronavírus elleni harchoz ígérnek pénzt) az üzenetben személyes adatokat, bankkártya adatokat kérnek a csalók. [1]

Instant üzenetküldő alkalmazás: Az általánosan elterjedt és használt okos mobileszközöknek köszönhetően rendkívül népszerű az ilyen jellegű alkalmazások használata. Ezeken keresztül a támadó online cseveghet, így bizalmába férkőzhet az áldozatnak. A cél itt is a személyes adatok megszerzése, ezzel pedig akár a felhasználó fiókjának a feltörése. Összetettebb támadás esetén hamis profil mögé bújva pénz utalásra is rávehetik az áldozatokat. De jellemző, hogy az ilyen üzenetek segítségével, akárcsak az sms üzenethez hasonlóan az üzenetben elhelyezett linkre kattintva rosszindulatú programok települhetnek eszközünkre, vagy adathalász oldalra irányíthatnak. [1]

Vishing: Csaló hívások, melyeket telefonon keresztül követnek el. Nem igényel technikai ismeretet, leginkább a manipulációs módszerek igénybevétele szükséges a sikeres támadás kivitelezéséhez. Alapja lehet egy későbbi, más technikát igénylő social engineering támadásnak is. A verbális kommunikációs csatornát kihasználva, ilyenkor általában személyes adatok, jelszavak, bankkártya adatok megszerzése a cél. A támadó valamilyen szervezet képviselőjének, hatóság munkatársának kiadva próbálja az adatokat megszerezni, például kötelező adategyeztetésre, központi rendszer újraindítása miatti ellenőrzésre, mobilkészülék vírusirtására, biztonsági ellenőrzésre, bankkártya tranzakciók, vagy adóvisszatérítés ellenőrzésére hivatkoznak. [1]

3-6. ábra: Gyakori IT alapú social engineering technikák [27]

Közösségi oldalak felhasználásával információgyűjtés: Fontosnak tartom megemlíteni, tekintettel, hogy gyakorlatilag nagyon egyszerűen, kis költséggel férhetnek hozzá nagy mennyiségű információkhoz, adatokhoz a támadók ezekről az oldalakról, kiindulópontot jelentve egy másik támadáshoz. Milyen információhoz is juthatnak hozzá? Személyes adatokhoz, helyinformációkhoz, üzleti információkhoz, információkhoz barátokról, munkatársakról, eseményekről, nyaralásokról, magán, vállalati ingatlanokról, ez lehet az oldalakon megosztott fotók segítségével is. Korábban ezek az információk nem, vagy csak nagyon nehezen voltak beszerezhetők. Felgyorsult világunkban kevés időbefektetéssel, könnyen összegyűjthetőek, egyre többet és egyre gyakrabban osztunk meg magunkról információkat a közösségi média felületeken, veszélyeivel mit sem törődve, és ezek rendkívül értékessé válhatnak rossz kezekben. De akár kártékony programok, egy üzenetben, link formájában történő csatolására is alkalmasak a közösségi oldalak. [1] [14] [27] [36]

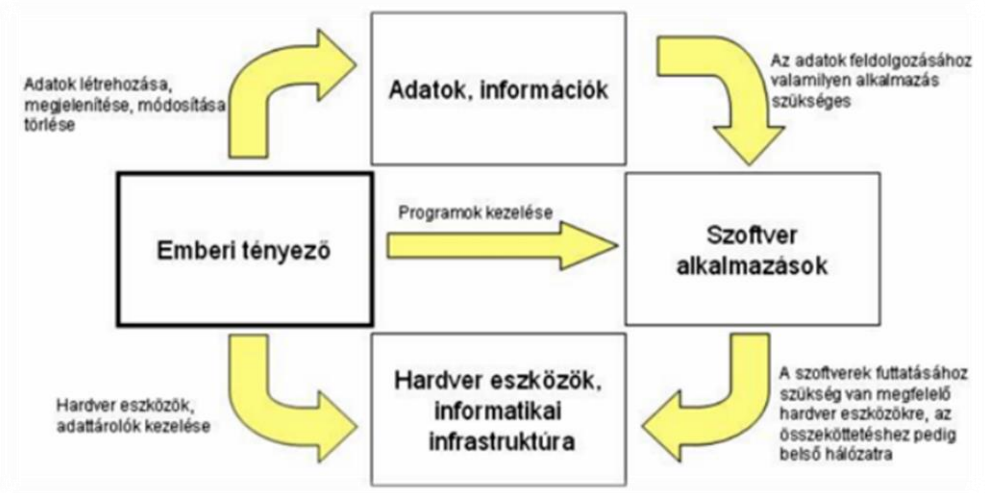
Pharming - DNS eltérítésen alapuló: Erős technika tudást igényel, azonban így egy átlagfelhasználónak nagyon nehéz dolga van, hogy kiszűrje. Két részből tevődik össze, a támadók létrehoznak egy hamisított, az eredetivel szinte azonos weboldalt, majd a DNS szerverek sérülékenységét kihasználva, az elérési útvonalat támadják, az eredeti weboldal domain nevének eltérítésével, a hamis weboldal IP címére irányítva az áldozatot. [1] [14]

Baiting - adathordozók szétszórása: Ez a technika társulhat humán alapon végrehajtott technikával is, amikor bejutunk az épületbe és egy tetszőleges adathordozón, például pendrive-on kártékony programot terjesztünk. Ilyenkor a támadó tetszőleges helyen, „véletlenül” elhagyja, szétszórja a fertőzött adathordozót, akár figyelemfelkeltő felirattal is ellátva, pl.: „bizalmas”, kihasználva az emberi kíváncsiságot, így a gyanútlan felhasználó bedugja a gépébe és már meg is fertőződött a gépe. [1] [13] [14] [37] A 3-6. ábra összefoglalva mutatja a legyakoribb IT alapú social engineer technikákat.

Bemutatása a számítógépes tudást igénylő támadásoknak szintén nem teljes körű, azonban így is láthatjuk milyen sok és mennyi fajta támadás létezik, akár keverve, egymásra építve felhasználva a különböző módszereket, esetleg kiegészítve a humán alapú támadási technikákkal. Ez alapján is megismerhettük mennyi veszély leselkedik a kibertérben a világhálót gyanútlanul, biztonságával kevésbé törődő, vagy azzal nem tisztában lévő felhasználóra.

4 BIZTONSÁG SZEMPONTJÁBÓL AZ EMBERI TÉNYEZŐK BEMUTATÁSA

A social engineering ahhoz, hogy sikeresen működjön, nem csak technika tudás, de gyakorlatilag valamifajta pszichológiai tudás, készség is szükségeltetik, vagyis jól kell bánni az emberekkel, és ismerni kell azokat az emberi tényezőket, kihasználható tulajdonságokat, amin keresztül sikeresen végre tudunk hajtani egy ilyen fajta támadást. Lefordítva, azt mondanám ahogy egy programozó kollégám fogalmaz: „A probléma legtöbbször a monitor és a szék háttámlája között helyezkedik el”. A felhasználók, akik működtetik a technikát, használják a hardvereket, a szoftvereket és természetesen ők azok, akik rendelkeznek, rendelkezhetnek a szükséges információval, és közvetlenül hozzáférhetnek a védendő információkhoz. Ezt a hatást mutatja be a 4-1. ábra. Azonban a legfontosabb, hogy rendelkeznek olyan kihasználható emberi tulajdonsággal, ami alapján a leggyengébb láncszemmé válnak a biztonság szempontjából, melyeket a támadó megpróbál kijátszani a károkozás, vagy a személyes, bizalmas információhoz való hozzáférés érdekében. [16]



4-1. ábra: Az emberi tényező hatása [38]

Az emberek olyan különféle tulajdonsággal rendelkeznek, amelyeket egy támadó könnyen kihasználhat és így potenciális célpontnak tekinthető. Ezek az alábbiak:

Segítőkészség: A legtöbb egyszerű humán alapú támadás erre épül, például a segítségkérés technikája is. Hiszen az emberekben alapvetően benne van a segítőkészség, a segíteni akarás, a támadó ezt egyszerűen kihasználhatja, csak megkérdezi a célszemélyt a kívánt információról.
Viszonzás: Elsősorban a segítség nyújtás technikája épül erre, a támadó akár előidézve a problémát segítségünkre siet, majd cserébe kér egy szívességet, és az emberek többsége igyekszik viszonozni a szívességet.

Hiszékenység, kíváncsiság: Az egyik legjellemzőbb tulajdonság, már csak empátiából is könnyen elhisszük, hogy egy új munkatárs kér tőlünk segítséget, miközben egy social engineering támadást szenvedünk el, észre sem véve, hogy kiadtunk fontos információkat. Kíváncsiság a mozgatórugója az adathalász támadásoknak, amikor rákattintunk az e-mail-ben lévő linkre, vagy megnyitjuk a csatolmányát, esetlegesen bedőlünk egy nyereményjátékot ígérő hamis weboldalnak, reklámnak.
Monotonitás, figyelmetlenség: Legtöbbször a rutin munkát végzőknél fordul elő, akár recepción, Helpdesk munkáknál. Figyelmetlenségből a dolgozó a hozzá érkező sok hasonló kérdésből, nem veszi észre egy támadó információszerzésre irányuló kérését. Figyelmetlenségből adódhat, hogy a dolgozó bizalmas információkat hagy az asztalán, vagy nem megfelelően megsemmisített, szintén bizalmas adatokat tartalmazó dokumentumokat dob a kukába, így könnyen célponttá válva. Ide sorolható a *hanyagság* is, amikor a munkavállaló, felhasználó, tudatosan, nem törődve, illetve figyelmen kívül hagyva az esetleges következményeket, szegik meg az információbiztonsági szabályokat.
Befolyásolhatóság: Meggyőzéssel, megvesztegetéssel, szélsőséges esetben megfélemlítéssel jut a támadó a számára releváns információkhoz. Kapcsolódhat hozzá az *elégedetlenség,* egy elégedetlen munkavállaló ilyen esetben jelentős károkat okozhat a szervezetben.
Biztonságtudatosság hiánya: Minden típusú támadás alapja lehet, ha a felhasználók nem ismerik a különböző technikákat, így felismerni sem fogják őket támadás esetén, és védekezni sem tudnak ellene, ilyen esetben észre sem veszik, hogy csalás áldozatává váltak. Ehhez kapcsolódó a *szakértelem hiánya,* ha valamit felületesen ismerünk, vagy tudásunk van róla, nem tudjuk megállapítani mely adatokat, információkat kezeljünk bizalmasan.
Fáradtság, túlterheltség: Ilyen esetben nagyon nehezen szűrjük ki a támadásokat, mind munkahelyi, mind otthoni környezetben, nem tudatosan rengeteg hibát is véthetünk, megsértve a biztonsági kritériumokat.
Fontos megemlíteni az *emberi természet hajlamait* is, melyeket az emberi pszichét jól ismerő támadók szintén könnyedén kihasználnak, céljuk elérése érdekében. Ilyen a *hatalom,* az emberek sokkal könnyebben hajlanak megtenni számukra kényelmetlen dolgokat, amennyiben az egy felettesüktől érkezik. Ide tartozik a *szeretet* is, az emberek könnyebben tesznek eleget olyan kéréseknek, melyek kedves emberektől érkeznek, melyet a támadó könnyen kihasznál, akár eljátszva, hogy azonos a hobbijuk, érdeklődési körük.
A *kölcsönösség* szintén fontos természeti hajlam, könnyen teljesítünk egy kérést, ha cserébe, ígérnek, vagy kapunk valami értékeset, vagy ha rajtunk segítenek, azt úgy érezzük viszonoznunk kell. Ide kapcsolódhat a szűkösség hajlama amikor könnyebben teszünk eleget olyan kéréseknek, amik valamilyen vélt, vagy valós előnyhöz juttatnak. Például amikor álweboldalak értékes nyereményt kínálnak regisztrációért cserébe.

Jelentős a *társadalmi megerősítés* hajlama is, ilyenkor az emberek nehézségek nélkül tesznek olyan dolgokat meg, ami összhangban van a többi ember cselekedeteivel. Ha a

támadó felhívja, alig észrevehetően az áldozat figyelmét, egy adott dologra, amit már rajta kívül többen is megtettek, gördülékenyebben fog a kérés jogszerűségében megbízni. Az előzőekben ismertetett emberi, pszichológia tényezők, viselkedési jellemzők bemutatása, megismerése, megértése, fontos, egyenesen nélkülözhetetlen, egy valós támadás felismerésében, elhárításában. [4] [38]

Szakdolgozatom további részeiben elsősorban, a social engineering technikákon belül az legelterjedtebb, hatékony támadási formára, az adathalász technikákra helyezem át a hangsúlyt, és veszem górcső alá. Pontosan azért, mert úgy gondolom a vizsgált korcsoport, az átlagos, mindennapi digitális világban tett látogatásakor, elsősorban, és túlnyomó részben, ennek a veszélynek lehet kitéve. Ha találkoztak, vagy találkozhatnak valamilyen támadással, a statisztikai egyezéseket is figyelembe véve, a legnagyobb százalékban adathalász technikával kerülhetnek kapcsolatba.

5 KUTATÁS

A biztonságtudatosság, a digitális kompetencia és a social engineering-re, különösen a számítógép alapúra való „fogékonyság”, kéz a kézben járnak, ezért a kérdőíves kutatásomat is ezek mentén készítettem el. Ezen okból a kérdőívet úgy állítottam össze, hogy két részből áll, az első részben, 43 kérdésből próbáltam felmérni a választott korcsoport a digitális ismereteit, mennyire biztonságtudatosak, mennyire van jelen náluk a biztonság, ha a kibertérről, a világhálóra való csatlakozásról van szó, és mennyire ismerik ezek kockázatát. A második részben azt vizsgáltam, hogy adathalász e-mail támadások formájában, felismerik-e a social engineering támadásokat, találkozhattak-e már ilyen jellegű támadással. Ennek érdekében összességében 12 különböző, valódi, vagyis legitim, és nem valódi, vagyis csaló, adathalász e-mail közül kellett választaniuk a kérdőívet kitöltőknek, eldöntve, hogy az adott levél melyik kategóriába tartozik, de minden esetben három lehetőség közül tudtak választani (valódi, legitim / nem valódi, csaló / nem tudom). Minden e-mail választás után arra kértem a válaszadókat, hogy indokolják is meg döntésüket, mi alapján választottak, különböztették meg a valódi és csaló adathalász leveleket, és végső soron milyen okok befolyásolták a választásukat A kérdőívben szereplő e-mailek majd mindegyike saját gyűjtés, a saját postafiókomból. A 12 e-mail üzenet közül 8 csaló, adathalász, és 4 üzenet valódi, legitim levél

Összességében a választott kutatás a bevezetésben már leírt hipotézisekre keresi a választ.

1. Ezen korosztály nem használ biztonsági programokat, nem ismeri, nincs felkészülve a veszélyekre, de találkoztak már social engineering támadással, adathalász levelekkel.
2. Azon személyek, akik nem változtatták meg alapbeállított Wifi jelszavukat, eszközeiket sem védik meg biztonsági szoftverekkel.
3. Ezen korosztály a jelszavakat papírra írva tárolja otthon, és ha tehetik a lehető legegyszerűbb karakterkombinációjú jelszót használják.
4. Azon személyek, akik bonyolult, nehezen megjegyezhető jelszót használnak, több helyen is használják ugyanazt a jelszót.

A kérdőív kiértékelése, és az ezekből kapott eredmények, várható összefüggések, hozzájárulhatnak, hogy javaslatokat, megoldásokat tudjak tenni a felmerült problémákra, úgy mint, hogy hogyan lehet növelni a korcsoport biztonságtudatosságát, esetlegesen milyen módon, módszerekkel csökkenthetőek a kibertérben a korcsoportnál felmerülő kockázatok.

A kérdőívet az 55 éves kor feletti, a digitális technikákat, világhálót használó korosztályból kikerülők töltötték ki, melyet a Google Forms alkalmazásban készítettem el. Az alkalmazás segítségével gyűjtöttem és értékeltem is ki a visszaérkezett válaszokat. A további elemzéseket, lehetséges összefüggéseket, az IBM SPSS Statistics 28.0 verziójú programjával végeztem. A kérdőívet vagy közvetlen email-ben, vagy a linkjének az

elküldésével juttattam el a tárgyalt korcsoporthoz. A kitöltésre 2021. november 15. napjától 2022. február 25 napjáig volt lehetőség. Összesen 50 darab érvényes kérdőív kiértékelésére volt lehetőségem.
A kérdőív kérdéseinek összeállításánál az alábbi forrásokat használtam fel: [5] [6] [7] [8] [39] [40]
Maga a kérdőív a mellékletben, de a lenti linken is megtalálható:
https://forms.gle/fFpifbHcMbrSLkfN7

Mindazonáltal a kutatásom nem tekinthető reprezentatívnak, a mintavétel nagy száma nem volt biztosított, azonban direktívák megállapítására használható.

5.1 Általános trendek

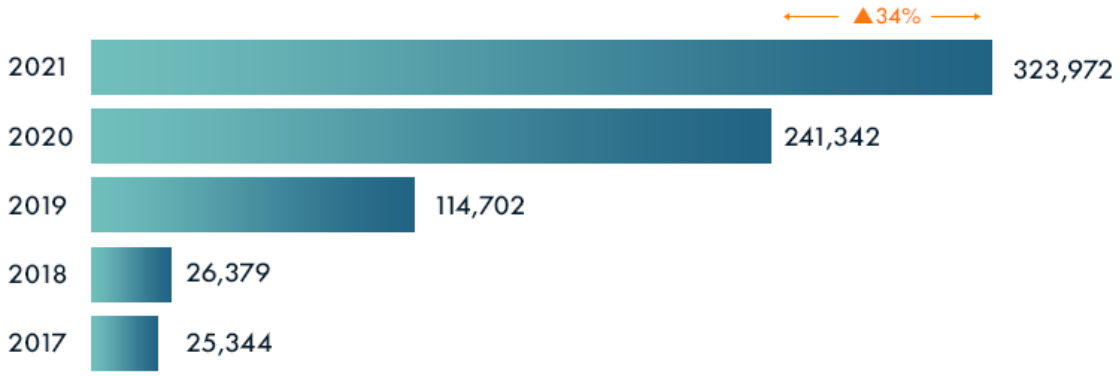
Fontosnak tartom, hogy bemutassak néhány általános felmérést, statisztikát, hogy lássuk, milyen mértékű, és mekkora veszélyt is jelenthet bizonyos social engineering támadási forma. Sokszor nem csak az egyének, de a vállalatok sincsenek felkészülve az ilyen jellegű támadásokra.

Az FBI felmérése alapján 2020-ban az adathalász támadás volt a leggyakoribb kiberbűncslekmény típus. Ezen incidensek száma megduplázódott a 2019-es 114.702 incidensről 2020-ban 241.324 incidensre. (5-1. ábra) Ez a szám 2021 nyarán az Anti-Phishing Working Group észlelése alapján elérte 260.642 incidens számot. Az adathalász-támadások 96%-a e-mailben érkezik, további 3% rosszindulatú weboldalakon keresztül, és mindössze 1%-ot telefonon keresztül hajtanak végre. Az adathalász támadások számának ilyen mértékű növekedése azt jelenti, hogy az e-mailes kommunikációs csatornákat ma már ellepik a kiberbűnözők. A Symantec kutatása szerint 2020-ban minden 4200 e-mailből 1 adathalász e-mail volt. A Google 2021. január 17-én 2 145 013 adathalászoldalt regisztrált. Ez a 2020. január 19-i 1.690.000-hez képest 27%-os növekedés jelent 1 év alatt. Az adathalász-támadások során veszélybe kerülő adatok három legfontosabb "típusa" a hitelesítő adatok (jelszavak, felhasználónevek, PIN-kódok), személyes adatok (név, cím, e-mail cím), majd az orvosi adatok következnek (kezelési információk, biztosítási igények). [41] [42]

5-1. ábra: Az adathalász támadások számának növekedése 2020-ban [43]

A 2020-as felmérések alapján, globális szinten a vállalatok mintegy 85%-a volt érintett phishing támadásban, és az adatvesztések 22%-a mögött phishing támadások álltak. Az átlagos felhasználók 97%-a nem volt képes felismerni egy jól felépített, szofisztikált phishing e-mailt, és a phishing levelek közel harmadát megnyitották a felhasználók, és 12%-uk rá is kattintott fertőzött linkekre, csatolmányokra. A ransomware-t tartalmazó phishing e-mailek aránya több mint 97%-ra tehető, és a sikeres social engineering támadások 77%-a adathalász e-maillel kezdődik. [44] [45]

Az FBI legutóbbi jelentése alapján (Internet Crime Report 2021) pontosabb képet is kaphatunk a vállalkozásokat és a személyeket fenyegető kiberbűnözésről. Az 5-2. ábra mutatja, hogy a különböző adathalász incidensek száma jelentősen megugrott az elmúlt öt évben, a 2020 és a 2021 év között 34%-os növekedést tapasztalhatunk. Kimagasló a ransomware támadások növekedése is, ez 2021-ben a riport alapján 3729 incidenst jelentett, mely 51%-os növekedés a 2020 évben mérthez képest. A zsarolóvírusok célba juttatásának három legfontosabb eszköze továbbra is az adathalász email-ek, távoli asztal kapcsolatok (Remote Desktop Protocol – RDP), valamint a szoftver sérülékenységek kihasználása. Az adathalász támadások számának növekedése mutatja, hogy a kiberbűnözők, továbbra is kihasználják, ki tudják használni az emberi psziché sebezhetőségeit, és így a kiberfenyegetések folyamatos kihívást jelentenek, minden a kibertérben megjelenő személynek. Továbbra is az emberi tényező, a legnagyobb kiváltó ok a kiberfenyegetések bekövetkezésének valószínűségében, ebből is következően, az e-mail még mindig az első számú fenyegetésvektor. [49] [47] [48]



5-2. ábra: Adathalász típusú incidensek számának növekedése [47]

E rövid kitérővel szerettem volna érzékeltetni, hogy napjainkban milyen nagyságú lehet egy IT alapú adathalász támadás, mely mértéke szerint, gyakorlatilag minden kibertérben megjelenő felhasználót érinthet. A statisztikákból is láthatjuk, az adathalász támadások száma évről évre növekszik, és egyre kifinomultabbak, így egyre nehezebben lehet majd megkülönböztetni őket a valódi üzenetektől. Belátható, hogy így mennyire felkészületlenül érheti azokat a személyeket akik nincsenek tisztában az őket fenyegető veszélyekkel, nem is gondolják, hogy bármiféle csalásnak áldozatai lehetnek. Mindezek alapján megállapítható, mennyire fontos, hogy foglalkozzunk ezekkel a problémákkal, és keressük a megoldásait.

5.2 Saját kutatás elemzése

Ebben a fejezetben leíró statisztikai összesítésként, a kérdőívre adott válaszokat, illetve azok arányát kívánom bemutatni.

Ha a nem szerinti megoszlást nézzük a kitöltők 65%-a nő és csupán 35%-a férfi. A korra adott válaszok már egyenletesebb eloszlást mutatnak, itt a válaszadók többsége az 55 és 65 éves kor között helyezkedik el, a legnagyobb arányban az 58 évesek képviseltetik magukat, a legidősebb válaszadó 77 éves.

A lakóhely szerinti megoszlás is egyenletességet mutat, a legnagyobb arányban, a községben és faluban lakók képviseltetik magukat (34%), melyet szorosan követ a fővárosban lakók aránya (31%), majd 21%-ban a kisvárosban lakók, és végül nagyvárosi, és megyeszékhelyen lakók (14%) következnek. Kitöltések alapján, tanyán egy válaszadó sem lakik.

A válaszadók iskolai végzettsége, már erős egyenletlenséget mutat, a legnagyobb arányban a főiskola vagy egyetemi diplomával rendelkezők vannak, ezek aránya 60%, őket követik a szakközépiskolai érettségivel rendelkezők (20%), majd a gimnáziumi érettségivel rendelkezők (12%). A legkevesebben a szakmunkásképzőt végzettek, (6%) és az OKJ vagy technikusi végzettséggel rendelkezők vannak (2%).

A kitöltők többsége (29%) az oktatásban, majd egyenlő arányban (12%), az egészségügyben, adminisztrációban, értékesítés, és a kereskedelemben dolgozik, dolgozott. Őket követi szorosan, szintén egyenlő arányban (10%) a közigazgatás, mérnök, műszaki, cégvezetés, és menedzsmentben dolgozók. Az informatika területén dolgozók aránya 8%.

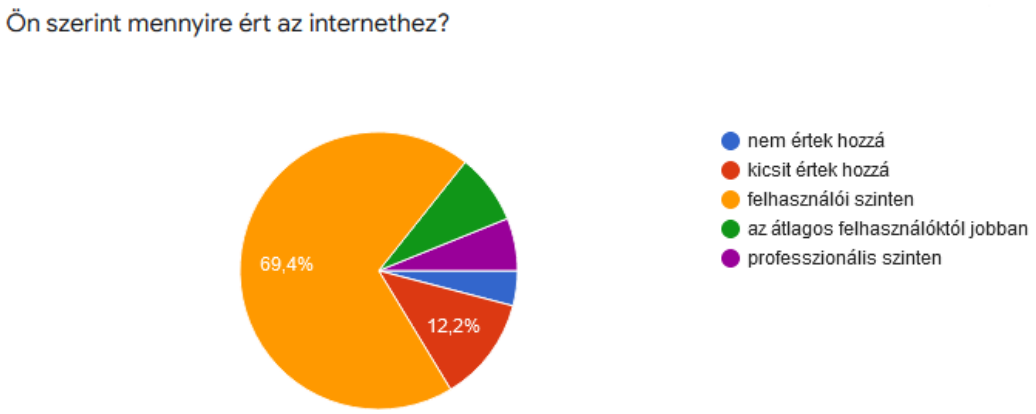
Az informatikai eszközök közül, talán nem meglepő módon, legtöbben okostelefonnal rendelkeznek (92%), ezt követi a laptop (80%), majd a számítógép (51%), és az okos háztartási és egyéb okos eszközök 31%-os aránya.

Ezzel szorosan összefüggve a leggyakoribb eszköz melyen interneteznek a mobiltelefon, melyet 36 fő, 74% választott, ezután következik a laptop, melyen 27 fő kitöltő (55%) szokott a leggyakrabban internetezni. Mivel itt több választ is meglehetett jelölni, a két leggyakoribb internetezésre használt eszköz között átfedés áll fenn.

Milyen gyakran használja az internetet kérdésre adott válaszban a megkérdezettek 61% válaszolta, hogy naponta internetezik, a másik leggyakoribb, hogy folyamatosan használják az internetet, ez az arány a válaszolók között 37%. Egy válaszadó csak különleges alkalmakor csatlakozik a világhálóra. Gyakorlatilag a válaszadók rendszeresen interneteznek, a mindennapi életük részévé vált, ez összefügg az okostelefonnal rendelkezők nagyszámú, 92%-os arányával.

Milyen tevékenységet végez az interneten válaszra a legtöbben, az e-mail-ek küldése, fogadása választ jelölték (92%). Ezután következik a hírek, cikkek olvasása (90%). Nagy arányban jelölték meg az internetes bankolást (67%), az ügyintézést (pl.: Ügyfélkapu) 65%. Az online vásárlást (pl.: élelmiszer, bútor, divatáru, elektronika stb.) a megkérdezettek 55%-a, az internetes vásárlás/eladás (pl.: eBay, Vatera, Jófogás) kérdést 39% jelölte meg. Jelentős arányban vannak akik chatelnek (61%), közösségi oldalon olvasnak, posztolnak (51%), vagy zenét hallgatnak (61%). Erre a kérdésre több válasz is megjelölhettek, így egyes válaszok között átfedés van.

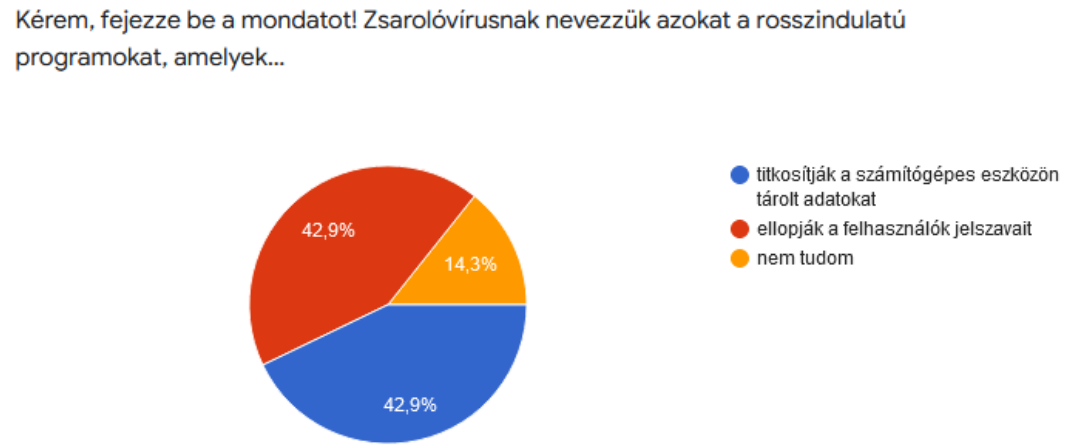
Arra a válaszra, hogy ítéljék meg mennyire értenek az internethez, a válaszadók 69%-a választotta, hogy felhasználói szinten értenek, 12% válaszolta, hogy kicsit ért, 8 % az átlagos felhasználóktól jobban ért hozzá, és 3 fő (6%) válaszolta, hogy professzionális szinten ért az internethez. (5-3. ábra)



5-3. ábra: Mennyire ért az internethez válaszolók aránya, Google Forms

A melyik szolgáltató tárol Önről adatokat kérdésre átfedésben 84% válaszolta, hogy az e-mail szolgáltatók, és 80% válaszolta, hogy a közösségi oldalak.

A kérdésre, hogy fejezze be a mondatot (zsarolóvírusnak nevezzük azokat a rosszindulatú programokat, amelyek…) a kitöltők 43%-a azt válaszolta, hogy ellopják a felhasználók jelszavát, és 43%-a válaszolta meg helyesen, hogy titkosítják a számítógépes eszközön a tárolt adatokat. Jókora arányban (14%) jelölték meg a nem tudom opciót is. (5-4. ábra)



5-4. ábra: Melyik rosszindulatú programot nevezzük zsarolóvírusnak, Google Forms

A választott korcsoportból a kérdőívet kitöltők 71%-a használ valamilyen ingyenes védelmi programot azon eszközein, melyeken internetezik, és 27% használ fizetős verziót. A nem használ válaszadást senki nem választotta, 1 fő nem tudja, hogy használ-e védelmi programot.

A válaszolók 84% nagyon fontosnak tartja, hogy legyen védelmi szoftver az eszközein, csupán 14% válaszolta, hogy kevésbé tartja fontosnak. A többi két opciót, a nem különösebben 1 fő választotta, és az egyáltalán nem választ, senki nem jelölte meg.

Vírusírtóval rendelkezők 39%-a rendszeresen, 22% szükség esetén frissíti a programot, a válaszadók 37%-nak magától frissül a vírusírtó program. Nem volt olyan, aki, a nem foglalkozom a frissítéssel lehetőséget választotta volna.

A jelszóhasználati kérdésekre adott válaszok szerint a legtöbben, (61%) 5 és 10 karakter hosszú jelszóval rendelkeznek, ezt követi a 10 és 15 karakter hosszú jelszóval rendelkezők aránya, mely 31% A 15 és 20 közötti jelszó hosszal 3 válaszadó, 20 karakter feletti jelszóval 1 fő, és. 1 és 5 karakter közötti jelszóval senki nem rendelkezik.

A válaszok átfedésével legtöbben (86%) olyan kombinációjú jelszót használ, melyben van szám, ezt követi (82%), az olyan karakterkombinációjú jelszó melyben van nagybetű is. A legkevesebben (32%), használ olyan jelszót, amelyben speciális karakter is van. Azok, akik mind nagy, mind kisbetűt, számot és speciális karaktert is használnak jelszavaik megválasztásánál az 19 fő, azok akik számot, nagy és kisbetűt használnak 24 fő.

A következő, még mindig a jelszóhasználati szokásokra érkező válaszok alapján a biztonságtudatosság kevésbé jellemző a kérdőívet kitöltőkre, tekintve, hogy nagy arányban, 41% százalék, csak szükség esetén változtat jelszót, 23% nem szokta megváltoztatni jelszavát, 10% ritkábban, mint évente változtatja meg jelszavát. Három kitöltő havonta, 4 fő minden gyanús körülmény esetén változtat jelszót. A visszaérkezett válaszok szerint, ugyanazt a jelszót 70% használja több helyen.

Hogyan jegyzi meg a jelszavát, hol tárolja őket kérdésre, a legnagyobb arányban, 53% válaszolta, a megtanulom fejben tartom opciót, és szorosan mögötte a felírja egy füzetbe vagy cetlire (47%) áll. Mivel erre a kérdésre több választ is meglehetett jelölni, így e két válasz között átfedés van, akik valahova felírják a jelszavukat, azok a legtöbb esetben meg is jegyzik, megtanulják azokat. Mindösszesen 3 fő használ a jelszavai tárolására jelszókezelő szoftvert.

Meglepő módon nagy azok aránya, (35%) akik jelszavát más is tudja, és 4% a nem válaszolok opciót választotta.

Előfordult-e Önnel, hogy kiadta a jelszavát válaszra, 6 fő válaszolt igennel, akik a rövid eset leíráshoz, az ügyintézéshez, a családon belül, és a munkahelyen munkaügyben kellett választ adták.

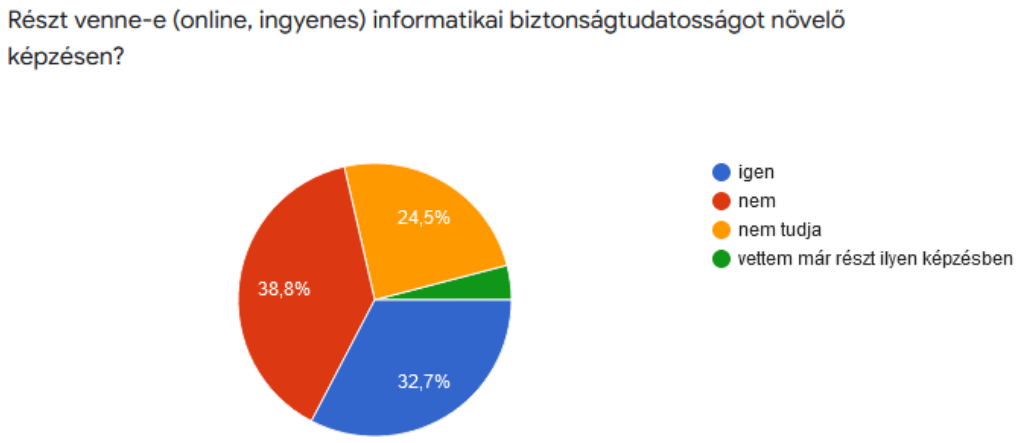
A válaszadók 61%-ának a legfontosabb, hogy a jelszava legyen könnyen megjegyezhető és biztonságos egyszerre. A legyen biztonságos lehetőséget 25% választotta. 15%-nak a legfontosabb, hogy a jelszava könnyen megjegyezhető legyen.

A válaszadók 27%-a nem szokott adatmentést készíteni eszközeiről, 25% csak bizonyos adatokról készít adatmentést, az évente, havonta, naponta lehetőséget egyaránt a kitöltők 8% választotta.

A legtöbben, vagyis 73% okostelefonjukon családi képet és videót tárolnak, ezt követi az e-mail cím (38%), majd a címek, naptárbejegyzések (23%) tárolása. Hárman orvosileleteket, két fő pénzügyi dokumentumot, 4-4 fő jelszavakat, személyes dokumentumokat is tárol okostelefonján.

A megkérdezettek több mint fele, vagyis 55% csak az ismert címről érkező mellékleteket nyitja meg e-mail üzeneteikben, 39% a levél tartalmától függően nyitja meg ezen csatolmányokat. A minden mellékletet, csatolmányt megnyitok opciót nem választotta senki, a soha nem nyitom meg, mert félek a vírusoktól lehetőséget 2 fő jelölte meg.

Ingyenes, online informatikai biztonságtudatosságot növelő képzésen meglepő módon a választ adók 39% nem venne részt, Ez annak függvényében is meglepő, hogy a válaszok alapján csupán két fő vett már részt ilyen képzésben. A részt vennének aránya 33%, de magas azok arány, (25%) akik nem tudják részt vennének-e ilyen képzésben. (5-5. ábra)



5-5. ábra: Esetleges képzésen résztvevők aránya, Google Forms

Arra a kérdésre, hogy mi okozza a legnagyobb nehézséget a számítógépkezelés, internetezés alkalmával eltérő válaszok születtek. Többen írták az angol nyelv hiányát, de megkérdezettek egy jelentősebb részének (13 fő) nincs olyan, ami nehézséget okoz. Voltak olyan személyek, akinek a biztonsági beállítások, a folyamatos változások követése, a hibaelhárítás, reklámok, táblázatok szerkesztése, online ügyintézés, változások követése, új programok, alkalmazások használata, vagy a jelszó megjegyzése okoz nehézséget.

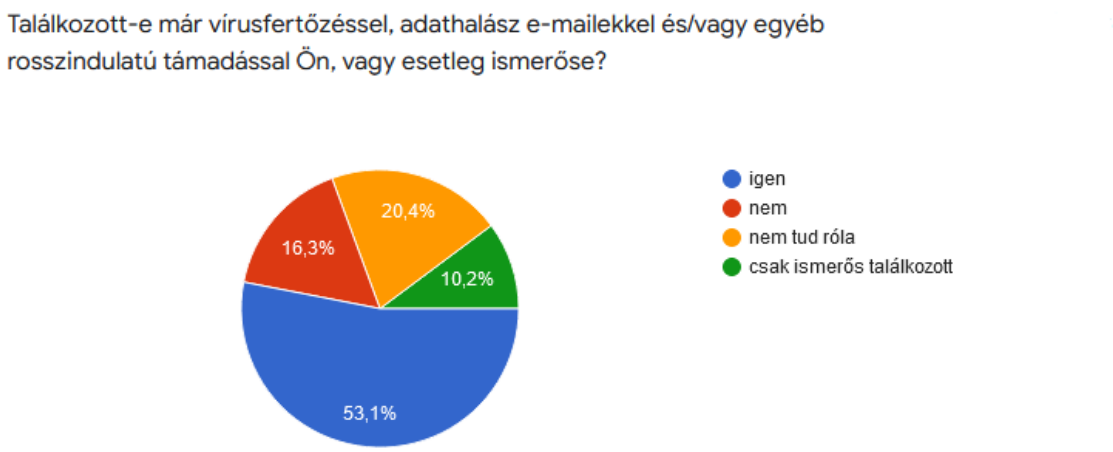
A milyen operációs rendszert használ kérdésre, Windows 10 operációs rendszert használ a kitöltők több mint fele (71%). A másik jelentősebb operációs rendszer, amit használnak az a Windows 7 (12%). 3 válaszadó nem tudta, hogy milyen rendszert használ, és akadt két fő, aki már Windows 11-gyel rendelkezik. Linux, vagy Mac Os senkinél sem fut. Az Operációs rendszer a kitöltők 49%-ánál automatikusan frissül, igen jelentős számban 21% nem frissíti az operációs rendszerét, de 22% frissíti azt. A válaszadók 8%-a pedig nem tudja, hogy rendszeresen frissíti-e az operációs rendszerét.

A legtöbben okoseszközeiken, adatvédelmi és biztonsági beállításnak a képernyőzárat használják, ezen személyek aránya 41%, 37% választotta, hogy felülvizsgálja a hozzáférési jogosultságokat, és letiltja azokat melyek nem szükséges a működéshez, 35% választotta, hogy nem módosítanak semmit, gyári beállítást használnak, azt, hogy a nem használt funkciókat kikapcsolják szintén 35% választotta. A legtöbben (8 fő) a képernyőzárat és a nem használt funkciók kikapcsolását jelölte be egyszerre.

Biztonsági frissítés a válaszadók 57%-ának automatikusra van állítva eszközein Egyenlő azaz 10-10% azok arány akik nem tudják milyen gyakorisággal telepítenek biztonsági frissítést, vagy akkor frissítenek, amikor már nem tudják rendesen használni az eszközt, és 12% választotta amikor kijönnek a frissítések, és van rá időm opciót. 2 fő volt, aki a válasza alapján, soha nem telepít biztonsági frissítéseket.

Otthoni routerén változtat-e az alapértelmezett beállításokon (pl.: WiFi jelszó) a biztonságért válaszra 39% jelölte meg a soha, 35% választotta a csak ha szükséges, 14% a nem tudom hogyan kell megváltoztatni, 10% választott a nem tudom mit kellene megváltoztatni, és szintén 10% mindig megváltoztatja opciót jelölte. Többen megjelölték egyszerre a soha, és a nem tudom, hogyan kell megváltoztatni, valamint a nem tudom, hogyan kell megváltoztatni, és a nem tudom, mit kellene megváltoztatni választ.

A kérdésre, hogy találkozott-e már vírusfertőzéssel, adathalász e-mailekkel és/vagy egyéb rosszindulatú támadással Ön, vagy esetleg ismerőse, a megkérdezettek 53%-a válaszolt igennel, ezt követte 21%-os arányban a nem tud róla válasz, valamint 16% nem találkozott, és 10%-nál csak ismerős találkozott ilyennel. (5-6. ábra)



5-6. ábra: Rosszindulatú támadással találkozók aránya, Google Forms

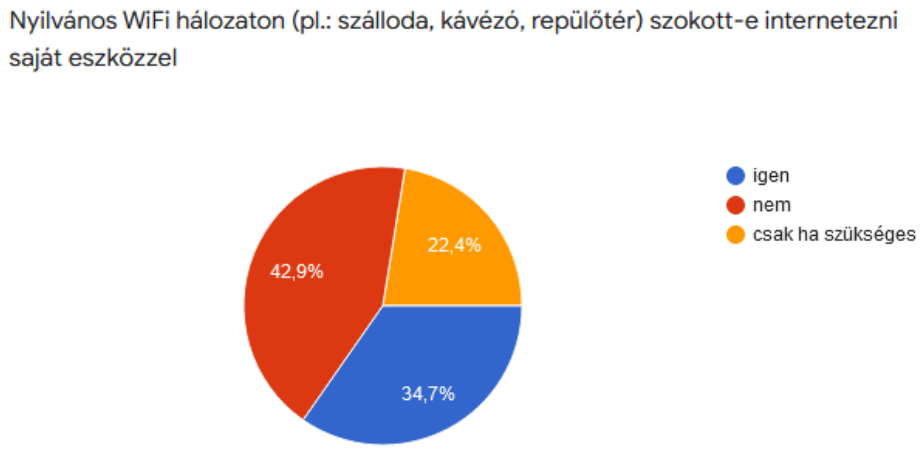
Nagy arányban 62% válaszolta, hogy biztonságtudatosabb lett, jobban védi az eszközeit, jobban odafigyel a biztonságra, miután, ő, vagy ismerőse találkozott rosszindulatú támadással, azonban nagy azok aránya is, 27% akik ezután sem tartották szükségesnek jobban odafigyelni a biztonságra.

A kérdésre, hogy előfordult már, hogy egy ismeretlen feladótól érkező elektronikus levél ajánlására látogatott meg egy weboldalt, töltött le valamit, rendelt meg valamit, vagy fizetett valamit, 92% a nem választ jelölte meg, és 8% válaszolt igennel.

A kétfaktoros hitelesítést a kitöltők 33%-a nem ismeri, 35% aki használja, de 14% azok aránya akik csak szükség esetén használják, és 8% a nem tudom választ jelölte meg. Jelszómenedzser programot a többség, 57% nem használ, 37% nem is ismer ilyen programokat.

A leggyakrabban, talán nem meglepő módon a Facebook-ot, mint közösségi oldalt látogatják, de volt olyan válaszadó, aki csak a munkája miatt használja Többen használják még a YouTube-ot, és 8 fő nem használ, nem látogat közösségi oldalakat. A közösségi oldalakon a leggyakoribb a családi, baráti képek megosztása, (25%) majd követi a családi állapot és kapcsolat megosztása, mely aránya 18%, és szintén 18% a képek földrajzi helyinformációval való megosztás aránya, személyes adatokat a válaszadók 10%-a oszt meg.

Nyilvános WiFi hálózaton (pl.: szálloda, kávézó, repülőtér) szokott-e internetezni saját eszközzel kérdésre a legtöbben, 43% nemmel válaszolt, 35% azok aránya, akik szoktak, és 22%-a kitöltőknek csak akkor használj a nyilvános WiFi hálózatot, ha szükséges. (5-7. ábra)



5-7. ábra: Nyilvános WiFi hálózatot saját eszközzel használók, Google Forms

Azon személyek, akik használják a nyilvános WiFi hálózatot, legnagyobb arányban 70% hírportálokat szoktak meglátogatni ekkor, de magas 28% azok aránya akik valamilyen online szolgáltatásba is bejelentkeznek ilyenkor.

A kérdőív második részé a csaló (8 db.) és legitim (4 db.) adathalász e-mail üzenetek megkülönböztetéséből állt, azon okból, hogy képet kapjunk arról, a válaszadók mennyire ismerik e támadási formát, mennyire fogékonyak rá, egyáltalán képesek-e megkülönböztetni a jogszerű e-maileket, a jogtalan üzenetektől. Minden válasz után

opcionálisan lehetőség volt indokolásra is, hogy esetlegesen megtudjuk mi az ami alapján ítélnek.

A leveleket a lenti (5-8. ábra) táblázatban foglaltam össze, a kérdőívben való bemutatásuk sorrendjében. A táblázat összefoglalja, hogy mi volt a bemutatott e-mail üzenetek tartalma, mik voltak a jellegzetes ismerettőjegyeik, és, hogy legitim, vagy csaló e-mail-ről volt-e szó.

E-mail	E-mail típusa	Ismertető jegy, megjelenés	E-mail tartalma
MVM Next	*nem valódi, csaló*	*link elhelyezése, kisebb nyelvtani hiba, címzett azonosítására felhasználói azonosító szám*	*hitelkártyás fizetés sikertelen*
repjegy.hu	*valódi, legitim*	*link elhelyezése, logók*	*repjegy utalvány ajándékozása*
Targetmax, PROAKTIVdirekt	*valódi, legitim*	*vizuális képi megjelenítés, link elhelyezése, levelező listáról leiratkozási lehetőség*	*nyeremény sorsoláshoz csatlakozás*
OTP Bank	*nem valódi, csaló*	*eredetivel megegyező logók, márkajelzés használata, feladó e-mail címe megtévesztő (info@otpdirekt.hu), link elhelyezése*	*tájékoztatás szolgáltatás megszünéssel kapcsolatban*
MVM Next	*nem valódi, csaló*	*több link elhelyezése, címzett azonosítására szerződéses folyószámla szám és számla szám*	*számla nem fizetés bankkártyás fizetéssel a linkre kattintva kiegyenlíthető*
NAV	*nem valódi, csaló*	*feladó e-mail címe nem látható, link elhelyezése, NAV eredeti lógójának használata*	*adóvisszatérítés*
Linux Akadémia	*valódi, legitim*	*link elhelyezése, a levél megjelenése a kérdőívben szereplő több csaló levélre hajaz*	*kvízkitöltés, nyereményhez kötve*
K&H Bank	*nem valódi, csaló*	*link elhelyezése, eredeti banki logó használata, feladó e-mail címe megtévesztő (info@kh.hu)*	*átutalás feldolgozás hiba*
MVM Next	*nem valódi, csaló*	*fenti címsor szerint lejárt villanyszámla, színes logók az eredetivel megegyezően, több link elhelyezése,* ***figyelmeztetés adathalászatra!***	*földgázszámla kiegyenlíthető*
ERSTE bank	*nem valódi, csaló*	*link elhelyezése, rendezetlen elrendezés*	*biztonsági rendszer frissítés*
Extreme Digital	*valódi, legitim*	*link elhelyezése, céges logó használata*	*E-mail cím megerősítésre vár*
Bitcoin fiók egyenleg	*nem valódi, csaló*	*link elhelyezése, rendezetlen elrendezés, nyelvtanilag nem megfelelő üzenet*	*fiók megerősítése bitcoin-hoz való hozzájutásért*

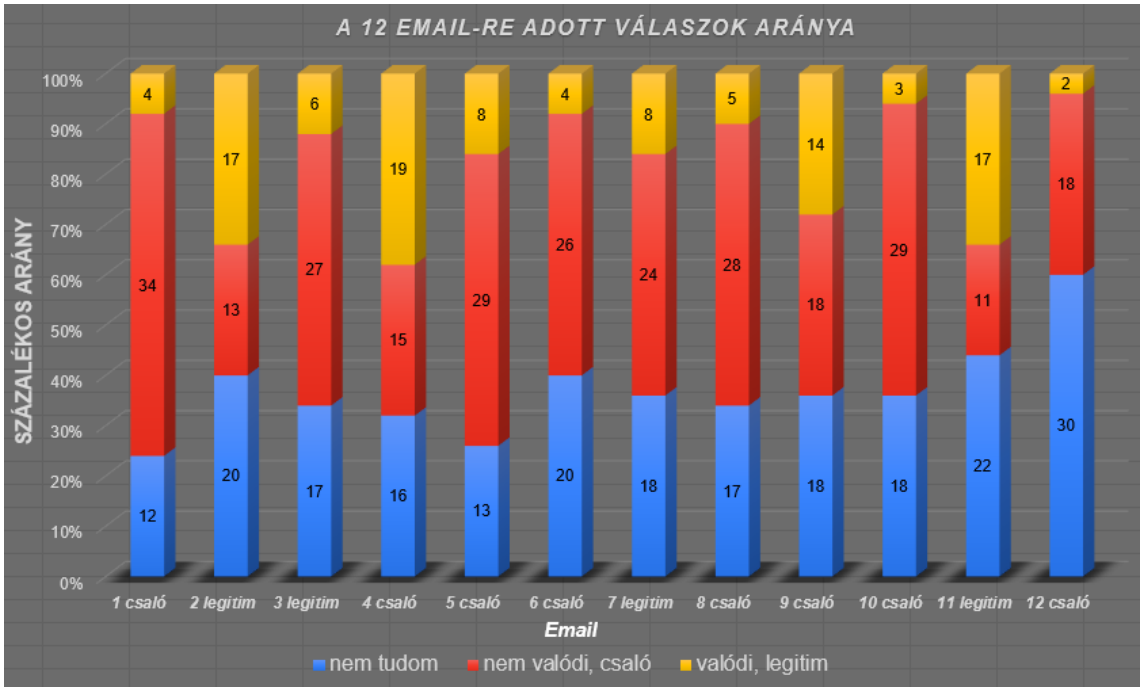
5-8. ábra: A bemutatott e-mail-ek jellemzői, szerző saját szerkesztése

Az 5-9. ábra megmutatja az összes e-mail-re leadott válaszok egyenkénti arányait.

A beérkezett válaszok alapján megállapítható, hogy amennyiben az e-mail valamennyire szofisztikált, a válaszadók nehezen tudják megkülönböztetni a valódi és hamis e-mail-t. Ilyen esetben, és általánosan is jellemző a nem tudom válaszok nagy százalékos aránya. Ami azt mutatja, hogy amennyiben az eredetivel szinte megegyező, vagy valamilyen azonos ismertetőjegyet, logót tartalmazó e-mailt kapnak, csupán a levél szövege, üzenetének tartalma alapján nem tudják eldönteni teljes bizonyossággal, hogy az adott levél legitim, vagy nem legitim.

Ezt legjobban a negyedik, OTP bankos csaló e-mail mutatja, ahol az eredetivel azonos jegyeket, logókat használtak a támadók, és a válaszadók aránya egyenlően oszlott meg,

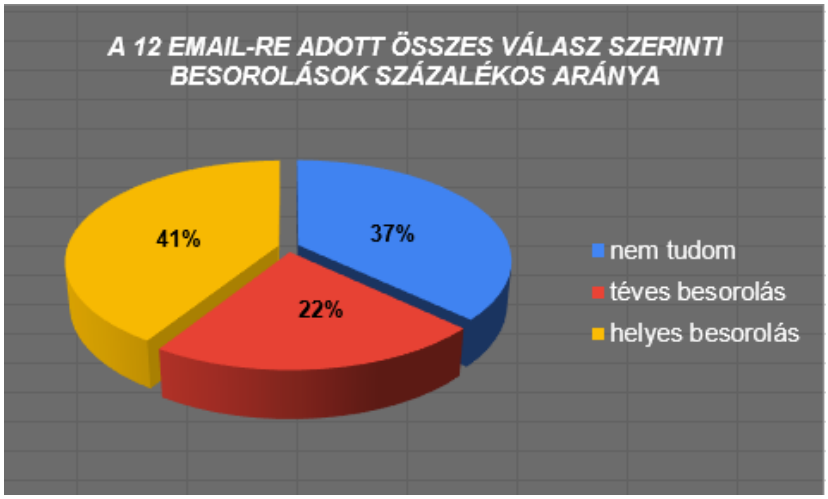
vagyis 16 fő nem tudta, 15 fő helyesen értékelte csalónak, de 19 fő legitim üzenetnek jelölte. Volt olyan válaszadó, aki az OTP bank saját hírlevelének hitte, vagy hivatalos értesítőnek, ahogyan volt olyan válaszadó is, aki szerint ilyen levelet nem küld a bank. Értékelés alapján nagyban növelheti is a bizalmat az olyan jellegű üzenet, ami vizuálisan jól megszerkesztett, az eredetivel megegyező vagy hasonló logókat, szimbólumokat használ. A kilencedik MVM Next csaló e-mail-re, amely vizuálisan a legjobban hasonlított az eredeti levélre, és még *adathalászatra is figyelmeztetnek* benne, itt 18 fő nem tudta eldönteni, szintén 18 fő helyesen, de 14 fő helytelenül ítélte meg az üzenetet.



5-9. ábra: Az egyes e-mail kérdésekre adott válaszok aránya, szerző saját szerkesztése

Volt olyan e-mail, a hetedik, a Linux Akadémia, ami valódi e-mail volt, azonban egyszerűen megfogalmazott, linket tartalmazó, logó nélküli üzenet volt, ami sokszor az adathalász e-mailek jellemzője, de egyéb gyanús dolgot nem tartalmazott, illetőleg a küldő e-mail címe is látható volt, ami egy abszolút legitimnek tűnő cím volt. Ezt a levelet 24 fő csalónak értékelte, és csupán 8 fő értékelte valóban legitimnek, a bizonytalanok aránya itt is nagy volt, 18 fő. A hármas PROAKTIVdirect legitim üzenetet csak 6 fő jelölte meg helyesen, és 27 fő csalónak, ami összefügghet a vizuális megjelenésével, ami hasonlóságot mutat a nem jogszerű e-mailekkel, ennek megfelelően nagy arányban, 17 fő nem tudta eldönteni, hogy hova sorolja. Kiemelkedő még a tizenkettedig Bitcoin levélre adott válaszok aránya, ahol 30 fő nem tudta eldönteni, hogy csaló, vagy legitim üzenetről van szó, pedig a levél megjelenésében, vizualitásában, a jogszerűtlen levelek formáját követi. Erre magyarázat lehet az ehhez én nem értek, nem ismerem a Bitcoint indokolások nagy száma, ami a korcsoportot nézve (nehezen követik a változásokat) talán nem is meglepő.

A válaszok alapján összeségében megállapítható, (5-10. ábra) hogy a kitöltők közel fele (41%) jól tudja megkülönböztetni a csaló és valódi üzeneteket. Azonban a válaszadók zavarodottságát mutatja, hogy a bizonytalanok aránya is hasonlóan magas (37%), melyhez társul, azon kitöltők 22%-os aránya akik tévesen sorolták be az üzenetek típusát.



5-10. ábra: E-mail kérdésekre adott összes válaszok aránya, szerző saját szerkesztése

Visszajelzést 25 fő hagyott hátra, mely alapján a legtöbben a feladó címe alapján döntöttek egyes levelek jogszerűtlenségéről, vagyis nem megfelelőnek, „kamunak" ítélték, továbbá sokan figyelték a magyartalan szövegezést és a helyesírási hibákat is. A banki leveleknél sokan indokolták a választást, azzal hogy „ilyen adatokat nem kérhet a bank", „pénzügyi adatokat kér, így nem hiteles". Voltak olyan kitöltők, akik a levél stílusa alapján próbáltak kategorizálni. Vizuális tényezőkkel, mint például logók, a válaszadók elhanyagolható száma indokolta választását, illetőleg ahol igen, ott a hivatalosnak tűnő márkajelzések, logók erősítették a legitimnek való megítélést.

Annak okán, hogy a felmérésemmel, még pontosabb képet kapjunk, a kérdőív átkódolásával, – az így kapott nominális változókkal – kereszttáblás statisztikai elemzéseket, próbákat végeztem, a már említett IBM SPSS programjával. Mindazonáltal szeretném előrebocsátani, hogy a különböző változók együttes vizsgálata esetén, a khi négyzet próba feltétele, az elméleti gyakoriság nem érte el a minimum 5%-ot, vagy egyes esetekben a egyes változók felülreprezentáltak voltak, így szignifikáns kapcsolatokat, összefüggéseket nem tudtam, vagy nem volt célravezető kimutatnom a pontatlanság, vagy a kutatási hiba magas valószínűségéből eredően. [49] [50] [51]

Mindezek ellenére úgy gondolom az eredmények következtetések levonására alkalmasak, és irányt mutathatnak további vizsgálatok, kutatások elvégzésére.

A kérdőív második részét kitevő vizsgálatnál, a kiugró értékekkel rendelkező leveleket (PROAKTIdirekt (3.), OTP Bank (4.), Linux Akadémia (7.), MVM NEXT ami a sorban a 9., és az utolsó a 12. Bitcoin fiók egyenleg tárgyú) elemeztem, úgymint, nem, iskolai

végzettség, internethez való tudás önértékelése, valamint a találkozott-e rosszindulatú támadás mátrixában, kiemelve a számunkra, releváns, vagy érdekes eredményeket.

A harmadik email-t vizsgálva a mennyire ért az internethez kérdés (tudás) változóval azok a személyek (35 fő), akik felhasználói szintre értékelték saját tudásukat, több mint fele 57% tévesen sorolta be az üzenetet, és magas volt körükben a bizonytalanok 34% aránya is. A magukat professzionális szintre értékelő 3 fő közül kettő, azaz 67% szintén tévesen ítélt. Az arányok hasonlóak a felhasználói szintű válaszolók esetében a négyes és hetes levelek esetében is, azonban itt a professzionális értékelésűek helyesen ítélték meg az üzenetek tartalmát. Az arányok a kilences és a tizenkettes emailek-nél változnak meg, a kilencest a felhasználói szintű válaszadók szinte fej-fej mellett ítélték valódinak 31%, csalónak 31% és 37% nem tudták megítélni, a kicsit értek hozzá tudásúak 50%-a, 3 fő szintén nem tudta megítélni. A tizenkettes email-nél azok akik kicsit értenek az internethez, a nem tudom aránya 83%, vagyis 5 fő, akik felhasználói szintre értékelték magukat, azok közel 69%-a, 24 fő szintén nem tudott dönteni az üzenetek megítélésénél.

Az összes email esetében, ha a nemek arányát nézzük, számottevő különbség nem mutatkozik, figyelembevéve azt a tényt is, hogy a kérdőíves válaszokban a nők aránya (33 fő) felülreprezentált.

Iskolai végzettséget tekintve (a legalacsonyabb iskolai végzettségű válaszadó a szakmunkás volt) az arányok szintén a hármas, négyes, hetes, kilences, és tizenkettes email-t vizsgálva, megegyezést mutatnak a „tudás” változó arányaival. Általában az iskolai kategóriákat vizsgálva, – kiemelve a kilences és a tizenkettes email-t – vagy azok aránya volt magas akik helytelenül ítélték meg az üzeneteket, vagy a bizonytalanok aránya, mely egyes esetekben elérte, vagy meghaladta az 50%-ot, így például a kilences email-nél, azok akik szakközépiskolai érettségivel rendelkeznek 60%-a nem tudom választ jelölte, viszont ennél az üzenetnél maradva azok akik gimnáziumi érettségivel rendelkeznek 83%-ban helyesnek ítélték meg, és a nem tudom választ nem is jelölték. A tizenkettes Bitcoin levélnél pedig akik főiskolai, vagy egyetemi diplomával rendelkeznek 63% közülük ugyancsak a nem tudom választ jelölte.

Az eredményekből látható, hogy azok akik legalább az internetes tudásukat felhasználói szintre értékelték, azon személyek bizonyos email-ek megítélésénél, nagy arányban voltak bizonytalanok, és úgyszintén, akik magas iskolai végzettséggel rendelkeztek szintén kiemelkedő volt körükben egyes email-ek esetén, a nem tudom jelölések aránya. Úgy gondolom e kimeneteleket, még akkor is érdemes figyelembe venni, ha látjuk, hogy a legtöbb üzenet esetén mind az internetes tudás, mind az iskolai végzettség változók tekintetében, a válaszadók több mint fele helyesen ítélt.

A találkozott-e már rosszindulatú támadással változó tükrében is végeztem statisztikai próbát az emailek-re adott válaszokkal. Ez esetben azok akik már találkoztak valamilyen támadással, nagy arányban helyesen ítéltek meg a leveleket, úgyszintén mint azok akiknek ismerőse találkozott ilyen támadással, és a bizonytalanok arány azok körében

volt magas, akik nem tudnak róla, hogy találkoztak-e már rosszindulatú támadással választ jelölték a felmérésben.

Mind a gyakorlati ismeretek, mind kutatások alapján megállapítható, hogy a jelszóhasználati szokások, a jelszó, mint hitelesítési eszköz, erős jelzése lehet a biztonságtudatosság mérésének. [11] Mindezért a kérdőívben több kérdésen keresztül is vizsgáltam e szokásokat, és ebből következőleg, nagyobb hangsúlyt fektettem a jelszavas változók vizsgálatára is.

Iskolai végzettséget tekintve minden egyes kategóriában győzött a legrövidebb 5-10 karakter közötti jelszó használat, legnagyobb arányban e jelszóhosszt használják. A nemeket tekintve nincsenek kiugró aránybeli különbségek a jelszó hossz tekintetében, a férfiak 53%-a, míg a nők 63%-a 5-10 közötti, a férfiak 35%-a, a nők 30%-a 10-15 karakter közötti jelszót használ. Míg 15-20 karakter közötti jelszavakat, a férfiak és a nők is 6%-a használja. A férfiak 70%-a, a női válaszadók 69%-a használja ugyanazt a jelszót több helyen is. Iskolai végzettséget nézve külön-külön kategóriánként, mindenhol 50%-ot meghaladó arányban használják ugyanazt a jelszót több helyen is. Azon személyek, akik professzionális szintre értékelték internetes tudásukat, nem használják több helyen jelszavukat, pontosan 50%-os arányt értek el azok, akik átlagos felhasználóktól jobban értik a netet, a többi önértékelési internetes tudás kategóriában, úgyszintén meghaladták az 50%-os arányt a több helyen jelszavukat használók. A milyen gyakran változtatja meg a jelszavát és az internetes tudás mátrixát vizsgálva, megállapítható, hogy azok akik nem értenek az internethez fele-fele arányban nem szokta megváltoztatni, és a csak ha a felület/alkalmazás kéri választ jelölték. A professzionális szinten lévők 66%-a minden gyanús körülmény esetén megváltoztatja a jelszavát, 33%-a viszont csak ritkábban mint évente. Az önértékelés alapján felhasználói szintű tudással rendelkezők 45%-a csak ha szükséges, 26%-a viszont nem szokta megváltoztatni jelszavát, a kicsit értő tudásúak 66%-a csak ha szükséges akkor változtat jelszót, és az átlagos felhasználótól jobb tudással rendelkezők, egyenlően 25%-os arányban, havonta, negyed évente, ritkábban mint évente, és végül minden gyanús körülmény esetében változtatnak jelszavaikon. Iskolai végzettséget nézve, szintén külön a kategóriákat, mindenhol a legnagyobb arányban a csak ha szükséges válasz kerekedett felül. A gimnáziumi érettségizettek körében ez az arány 83%-ot ért el, a diplomások között viszont csupán 30%-ot, a nem szokta megváltoztatni 20%-a mellett.

A nem és a védelmi programot, vírusirtót használók változó vizsgálata alapján megállapítható, hogy a férfiak 47%-a, míg a nők csupán 15%-a használ fizetős védelmi, vírusirtó programot. Ez a női válaszadók nagy száma (33 fő) alapján meglepő eredmény, ugyanakkor szignifikáns kapcsolatot vizsgálni ez esetben sem tudtam. Bár a nagy különbséget eredményezheti a férfiak nagyobb érdeklődése a technikai dolgok, újdonságok iránt. Az ingyenes informatikai biztonságtudatosságot növelő online képzés, és a lakóhely változó vizsgálata alapján a fővárosiak 63%-a részt venne, a kisvárosban élők 50%-a nem venne részt, és a nagyvárosban élők egyaránt 29-29%-a nem venne részt,

vagy nem tudja. Az eredmény abból a szempontból meglepő, hogy pont a fővárosiaknak van több lehetőségük különböző képzéseken részt venni, mégis ők választották a legnagyobb arányban, hogy részt vennének online biztonsági képzésen. Online képzés változó az iskolai végzettség tekintetében egyenletes elosztást mutat. Külön nézve a végzettségeken belül szinte egyenlő arányban oszlanak meg, azok akik részt vennének és azok akik nem vennének részt biztonsági oktatáson. A nem tekintetében a férfiak 53%-a, míg a nők csak 30%-a nem szeretne képzésben részt venni. A fizetős védelmi programot használó válaszadók 8%-a nem tudja, hogy találkozott-e-e már rosszindulatú támadással, azon válaszadók közül akik ingyenes védelmi programot használnak 22%-a nem tudja találkozott-e támadással, az az 1 fő aki nem tudja használ-e védelmi programot, nem is tudja találkozott-e már rosszindulati támadással. Előbbiekből következőleg feltételezhető, hogy azok, akik fizetős védelmi programot használnak, jobban oda figyelnek az esetleges rossz szándékú támadásokra.

Az előző különböző változók kereszttáblás vizsgálatai, eredményei alapján megállapítható, hogy a korcsoport körében szükséges lenne a digitális térben jelenlévő veszélyek, és fenyegetettségek minél nagyobb arányú tudatosítása, és ennek kockázataira való felhívására.

5.3 Hipotézisvizsgálat

1. *Ezen korosztály nem használ biztonsági programokat, nem ismeri, nincs felkészülve a veszélyekre, de találkoztak már social engineering támadással, adathalász levelekkel.*

A felmérésben résztvevők nagy aránya (71%) használ valamilyen védelmi programot, további 27% fizetős programot használ, valamint 84% tartja fontosnak, hogy legyen védelmi szoftver eszközein, de a válaszadók, több mint fele (53%) találkozott már valamilyen rosszindulatú támadással. Mely alapján a felvetésem első fele nem bizonyult igaznak.

2. *Azon személyek, akik nem változtatták meg alapbeállított Wifi jelszavukat, eszközeiket sem védik meg biztonsági szoftverekkel.*

A kitöltők közül 48 fő használ valamilyen védelmi programot, és 19 fő soha nem változtatja meg Wifi jelszavát, valamint 7 fő nem tudja hogyan kell megváltoztatni, és 5 fő nem tudja mit kellene megváltoztatni, azonban e válaszadók között átfedés van, így ezen a hipotézisem nem bizonyult igaznak a válaszadók körében.

3. *Ezen korosztály a jelszavakat papírra írva tárolja otthon, és ha tehetik a lehető legegyszerűbb karakterkombinációjú jelszót használják.*

Felmérésem alapján a kitöltők közül 23 fő (47%) válaszolt, hogy a jelszavakat papírra írva tárolja, emellett, többen jelölték párhuzamosan, hogy megjegyzi megtanulják, ellenben senki nem használ 1 és 5 közötti karakterkombinációjú jelszót, valamint ahogy

a felmérés leírásában rámutattam, azok, akik mind nagy, mind kisbetűt, számot és speciális karaktert is használnak jelszavaik megválasztásánál 19 fő, azok, akik számot, nagy és kisbetűt használnak 24 fő. Az előzőek alapján kijelenthető, hogy ezen felvetésem sem bizonyult igaznak, azok között, akik a kérdőívemet kitöltötték.

4. *Azon személyek, akik bonyolult, nehezen megjegyezhető jelszót használnak, több helyen is használják ugyanazt a jelszót.*

Ugyanazt a jelszót 69%, vagyis 34 fő használja több helyen, akik mind nagy, mind kisbetűt, számot és speciális karaktert is használnak jelszavaik megválasztásánál 19 fő, és 10 és 15 közötti karakter hosszú jelszót 15 fő használ, mely kitöltők között átfedés található, ez alapján megállapítható, hogy utolsó felvetésem igaznak bizonyult.

5.4 Következtetések

A kérdőív kiértékelése alapján összességében megállapítható, hogy a vizsgált csoport körében fontos lenne a biztonságtudatosság növelése, kompetenciájuk bővítése. Ezt többek között mutatja a jelszóhasználatra vonatkozó kérdésre adott válaszok, valamint azon bizonytalanok magas arány is, akik nem tudták eldönteni a kérdőívben szereplő levelekről, hogy azok adathalász, vagy legitim üzenetek-e. Továbbá a válaszok értékeléséből konstatálhatjuk, hogy a kérdéses ismeretek növelésére, bővítésére a megkérdezettek körében nagyfokú igény is mutatkozik.

Megállapítható, hogy a fenyegetettség jelen van, és fenn áll a korcsoportnál, a kiberbiztonsági veszélyeknek markánsan kitett felhasználókról beszélhetünk, melyet jelez azon megkérdezettek (53%) magas aránya akik már találkoztak rosszindulatú támadással, valamint azok aránya is (21%) akik a nem tudnak választ adták arra, hogy találkoztak-e már ilyen veszéllyel, ami feltételezheti, hogy talán nincsenek is tisztában milyen kockázatokkal találkozhatnak, mikor a kibertérhez csatlakoznak.

Tekintve, hogy a korcsoport hiányos ismerete által veszélybe kerülhetnek olyan felhasználók is akik odafigyelnek a biztonságra, – gondoljunk egy munkahelyre, vagy akár csak egy otthoni hálózatra – ezért össztársadalmi szinten is fontos, hogy növeljük az idős korúak digitális ismereteit, fejlesszük online biztonságtudatosságukat. Ebből következőleg javasolt lehet központilag is kezelni a problémát, általános ajánlásokat megfogalmazni, online biztonságtudatosságot növelő tréningeket tartani.

Hipotéziseim felállítása és a kérdőívekre adott válaszok vizsgálata alapján azonban elnagyolt megállapítás lenne, hogy az idősebb korú internethasználók teljesen felkészületlenek lennének a kibertér veszélyeire, és digitális ismereteikhez kapcsolódó biztonságtudatosságuk sem lenne, bár ennek magyarázatára szolgálhat a magas iskolai végzettségű kitöltők felülreprezentálása. Ugyanis a válaszadók 59%-a főiskolai, vagy egyetemi diplomával rendelkezik, így ennek a kérdésnek az egyöntetű eldöntése, további kutatás tárgyát jelenthetné.

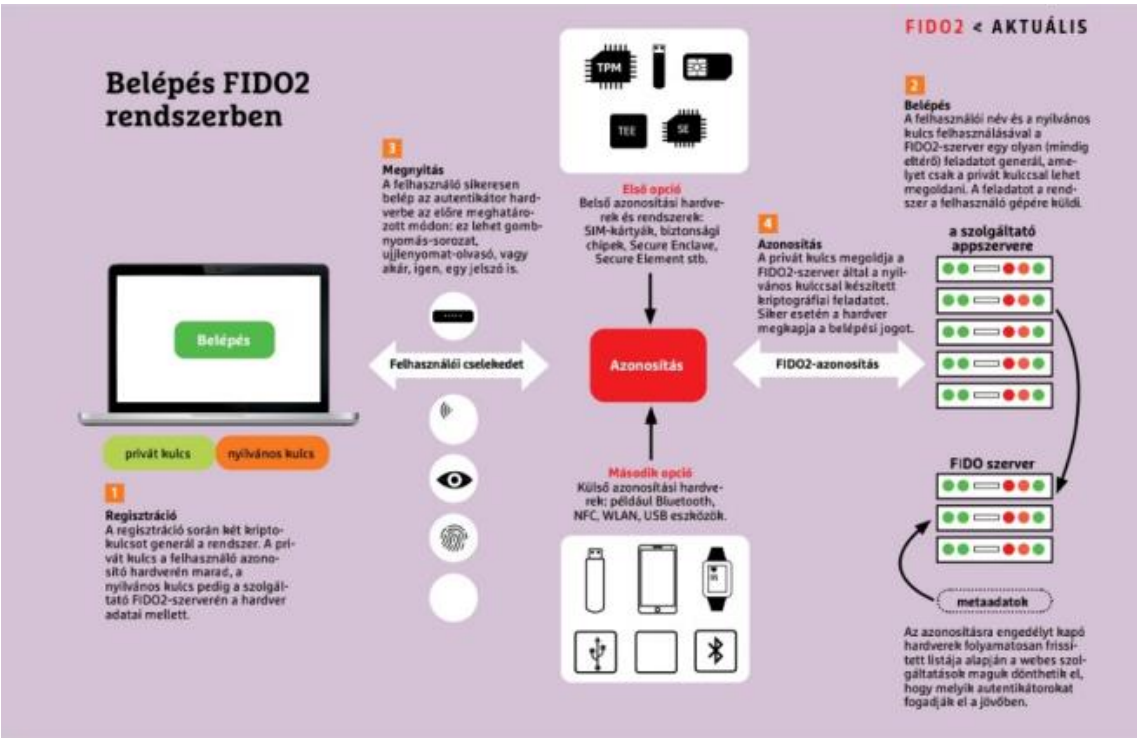
A fejezetben a kérdőíves felmérésem vizsgálatát, eredményeit mutattam be, kitérve a hipotézisvizsgálatra, és konklúzióinak levonására.

6 MEGOLDÁSOK, JAVASLATOK

Ebben a fejezetben megpróbálok megoldásokat találni, bemutatni, javaslatokat megfogalmazni a felmerült, elsősorban az adathalász támadásokkal kapcsolatos problémákra, – milyen megoldásokkal csökkenthetőek a kockázatok, hogyan növelhető a korcsoport biztonságtudatossága, és milyen módszerek, technikák segíthetnek a védekezésben, a veszély elkerülésében – figyelembe véve a kérdőív értékelését is. Valamint egy fejezetet szentelek egy összefoglalónak azzal kapcsolatban, – elsősorban adathalász levelekre kihegyezve – hogy a korcsoport mire figyeljen, mi alapján hozhatják meg döntéseiket, amikor egy számukra ismeretlen linkre kattintanak, vagy gyanús e-mailt nyitnak meg. Az emberi tényező, – még ha tudjuk is csökkenteni a kockázatát – mindig szerepet fog játszani a social engineering technikák alkalmazásának a sikerességében, ezért fontos, hogy technológiai módszereket bevetve is tudjuk akadályozni a fenyegetettségek bekövetkezését, elkerülését.

Felmérésemben a jelszóhasználati szokásokat feltárva megállapítható volt, hogy a jelszóváltoztatás esetében a biztonság kevésbé fontos a válaszadóknak, tekintve a 41%-os arányt, akik csak szükség esetén változtatnak jelszót. Bár a legtöbben fejben tartják és megjegyzik a jelszavukat, de 47% azok aránya, akik füzetbe, cetlire is felírják. Ebből is következtetve, ugyanazt a jelszót a megkérdezettek 70% használja több helyen, ezáltal veszélyeztetve azt, hogy egy szolgáltató feltörése, magával hozhatja a többi feltörését, és ily módon biztosítva több érzékeny adatunkhoz való hozzáférést. Azonban létezik olyan technikai megoldás ami jelszónélkülöséget hozna el, és gátat szabhatna az adathalász típusú támadásoknak.

Az úgynevezett FIDO2 szabvány, működési protokoll elterjedésével nem lesz szükség jelszó használatára az azonosításhoz, és az autentikáció során semmilyen érzékeny adat nem utazna a felhasználó és a szolgáltatás, (web)szolgáltató között. Ezzel a megoldással a phishing támadásoknak is elejét lehetne venni, ugyanis a módszerből adódóan az álweboldal nem rendelkezne a nyilvános kulcsunkkal és a hardver információinkkal, további előnye, hogy a biztonságos azonosítás használata egy egyszerű API-n keresztül megvalósítható.



6-1. ábra: A FIDO2 szabvány működése [52]

Bármiféle különleges felhasználói beavatkozás nélkül, a jelszó beírása helyett, egy titkosított folyamaton keresztül történik az azonosítás, mely kapcsolatot elég egyszer létrehozni, és onnantól a felhasználót a weboldal, online szolgáltatás, egy hardver elemhez köti (pl.: laptop, PC, USB kulcs, ujjlenyomat olvasó). Így maga a használandó eszköz fogja képviselni a kétfaktoros azonosítást. A 6-1. ábra ennek a folyamatát mutatja be. Legelőször az eszközhöz tartozó személynek kell elindítani a belépési műveletet, mely kizárja a hackelést, a távoli hozzáférést. Ezt követi az azonosítás, mely kizárólag közvetlenül az eszközön történik (pl.: ujjlenyomat olvasó), így a két végpont között nem mozog olyan adat, amit ellehetne lopni. Működését tekintve, felhasználónevet, és egy választott hardvert kell regisztrálni, mely folyamat során aszimmetrikus kulcsú titkosítási eljárással létrejön egy nyilvános kulcs, mely a szolgáltatónál marad a regisztrált hardver információkkal együtt, illetőleg a művelet során létrejött privát kulcs a felhasználó gépén marad. Ezt követően, ha a felhasználó belép a szolgáltatásba, weboldalra, az felismeri az azonosításra regisztrált hardvert, és kéri a következő azonosítást, például egy ujjlenyomatot. „Ha ez sikeres, jöhet a háttérben zajló, villámgyors, és tényleges azonosítás: a szerver a nyilvános kulcs alapján generál egy titkosított feladatot, amit kizárólag a felhasználó a hardverén tárolt privát kulccsal lehet megoldani. A sikert követően a készülék, és vele együtt a felhasználó bejut a rendszerbe, pedig az ő szempontjából a belépés gombra kattintás után csak egy extra, ma is sok helyen működő azonosítási lépést kell megtenni. Mivel minden szolgáltatónál minden hardver új kód-párt generál, ezek sosem ismétlődnek, ráadásul a jelszavas rendszertől eltérően semmilyen érzékeny titok nem utazik a felhasználó és a szolgáltató között”. Talán hamarabb

elhagyhatjuk a jelszavakat, mint azt gondolnánk. A nagy techóriások, a Google, az Apple és a Microsoft úgy döntöttek, jövő évben a platformjaikat (Android és Chrome; iOS, macOS és Safari; Windows és Edge) kompatibilissá teszik a FIDO jelszómentes szabványokkal. [52] [53] [54] [55]

Bekívánom mutatni Nyikes Zoltán által kidolgozott Internetes Vészhelyzeti Segélyhívó Rendszert is, melynek bevezetése különösen hasznos, és kívánatos lenne az általam vizsgált korcsoport körében. Ennek megerősítésére szolgálhat kutatásom is, mert mint ahogy már említettem, arra a kérdésre, hogy mi okozza a legnagyobb nehézséget a számítógépkezelés, internetezés alkalmával, a válaszok között a biztonsági beállításokat, , a hibaelhárítást, online ügyintézést, a folyamatos változások követését, vagy az új programok, alkalmazások használatát is említették. Továbbá Nyikes rámutat, és ez különösen igaz a vizsgálat csoportra, hogy jelenleg nincs olyan megoldás, ami informatikai biztonsági esemény bekövetkezésekor védelmet nyújthatna a felhasználóknak. A Segélyhívó Rendszer internetes zaklatás, vírustámadás, működési zavar, rendszerhiba, vagy rendszerösszeomlás esetén valós idejű azonnali megoldással segítené a bajba jutott felhasználókat. Üzemelése a vész, illetve segélyhívó rendszerek modelljét követné, diszpécser központtól a felhasználó azonnali technikai segítséget tudna kérni a fent felsorolt problémák megoldására, vagy akár ha az eset megkívánja, rendőrségi, nyomozati tevékenység is indíthatóvá válna. A Rendszert a meglévő 112-es Segélyhívó diszpécser központokba lehetne integrálni, vagy a Nemzeti Kibervédelmi Intézet alá, de akár önálló szervként is működhetne. Működését tekintve, „vészhelyzet esetén egy gombnyomásra, olyan dedikált virtuális magán hálózat kerülne használatra, amely előre definiált és elkülönített porton és csatornán lépne kapcsolatba a diszpécserközponttal, távsegítség nyújtásra és a rendszer helyreállítására.” Egy ilyen rendszer alkalmazására a jövőben talán még nagyobb szükség lenne, ha figyelembe vesszük IoT eszközök használatának növekedését, – az önvezető autók alkalmazásáról nem is beszélve – melyből következőleg a felhasználók az internet által egyre jobban ki lesznek téve a támadásoknak. [5]

A technikai jellegű megoldásoknál maradva, említést tennék a napjainkban is folyó kutatásokról, melyek folyamatosan fejlődve, egyre jobb és jobb eredményeket érnek el, ez pedig a mesterséges intelligencia használata az adathalász e-mail-ek felismerésére. A kutatások kiinduló pontja, hogy az adathalász levelek észlelésében nem hagyatkozhatunk csupán az emberre, akit könnyen lehet manipulálni, hanem automatikus adathalász felismerő mechanizmusok, programok kidolgozására van szükség, annak érdekében, hogy minél hatékonyabban vehessük fel a harcot a kiberbűnözőkkel. E célok elérésében a legnagyobb akadályt az jelentette, hogy a hagyományos módszerekkel a számítógépek nem voltak képesek megérteni az emberi kifejezésmódot. Azonban a mesterséges intelligencia, a gépi tanulás, és a természetes nyelvi feldolgozásnak köszönhetően napjainkban áttörés következett az adathalász levelek felismerésében, mely által jelentősen nőt az észlelési pontosság is. Egészen odáig, hogy egyes kísérletekben az

adathalász e-mailek felismerése 98,2% magas pontossági arányt produkált. A jövőben a veszélyek elhárításában és kiszűrésében, a mindennapok részeként is jelentős segítséget fognak nyújtani a kidolgozott mechanizmusok, programok, ezáltal eredményezve javulást, az adathalász jellegű támadások kivédésében, csökkentésében. [56] [57] [58]

Ma már mindenki részéről nyitott a lehetőség, hogy valamelyest hozzájáruljon ahhoz, hogy az internetes csalásokkal kevesebb embert érhessenek el a bűnözők. A Google Chrome böngészőjében olyan bővítményt telepíthetünk melynek segítségével jelenthetjük az ártalmasnak vélt oldalakat. A bővítmény (Suspicious Site Reporter) használatával, néhány kattintással tudjuk jelzésünket elküldeni a Google részére. Amennyiben bebizonyosodik, hogy valóban egy ártalmas weboldalról van szó, a techóriás hátrébb sorolja, vagy törli a webcímet a találati listákról, így segítve másokat, hogy ők már ne tévedhessenek a csaló oldalra. [59]

Fontosnak tartom, hogy a kibertérben leselkedő veszélyekre, és az azok elleni védekezésre, a hagyományos és digitális médiafelületeken, akár országos kampány keretében is felhívjuk a lakosság, és így a vizsgált korcsoport figyelmét. E hagyományos felületek széles elérési utat jelentenének, ezen idős korosztály részére. Ez látható például a Nemzeti Kibervédelmi Intézet (6-2. ábra) honlapján található színes, figyelemfelkeltő, rövid, és lényegletörő szórólapjain is. Ezek a kampányok ha széles körben terjednének, nagy mértékben alkalmasak lehetnek az adathalászat, és egyben a kibertér veszélyeinek tudatosítására.

6-2. ábra: Pszichológiai befolyásolás – védekezés a csalások ellen NKI szórólap [60]

Peter Coroneos tanulmánya szerint az emberi viselkedés alapjait újra megkellene vizsgálni, és mint a kiberkockázat kontextusban tanulmányozni, ezzel visszautalva a négyes fejezetemre, ahol az emberi tényezőt mutattam be a biztonság szempontjából. Coroneos szerint az emberi evolúció következtében a digitális világ veszélyeit máshogy érzékeljük mint a fizikai valóságét. Az evolúció során a kialakított védekezési mechanizmusainkat a látható és érzékelhető dolgok alakították, ezzel szemben a kibertérben, ami nem kézzelfogható, nincs látható és érzékelhető, vagy nem egyértelmű, a veszély, így kevésbé érzékeljük a fenyegetettséget, ezért nem is jut érvényre bennünk a kockázat/következmény dinamika. A veszélyek elkerülésére olyan viselkedést kellene használni az embereknek ami még nem fejlődött ki. „A tudatosság és a viselkedésbeli változás közötti kapcsolat a kockázati cselekvés és a kockázat következménye közötti közelség hiányának függvénye." A tudás arról, hogy milyen veszélyeket kell elkerülni, elválik a cselekvéstől. Nem elég a tudatosság növelése a figyelemfelkeltés az online viselkedés megváltoztatásához. Mindezek magyarázhatják, hogy bizonyos felhasználók, többek között miért dőlnek be a csalásoknak, kattintanak adathalász levélre, vagy adnak meg személyes adatokat a közösségi oldalakon. Tovább bonyolítja a helyzetet, – amellett, hogy a már bemutatott emberi tényezőket a kiberbűnözők sikeresen kihasználják – hogy a felhasználók agya biológiai szempontból különböző életkorban más válaszokat ad, például kamaszkorban az erős kockázatvállalás, és a hirtelen impulzusok jellemzik, míg felnőtt korban az agy könnyebben old meg bizonyos feladatokat. Ebből következőleg az internetezőkre nem lenne szabad homogén csoportként tekinteni, így (biztonság)tudatosságukat, kockázatkezelésüket is szükséges lenne eltérően, más módszerekkel tudományosabb alapon tréningezni, visszatérve az emberi viselkedés fundamentumaihoz, a minél nagyobb hatékonyság, és az erőforrás pazarlás elkerülésének érdekében. E kiberkockázati viselkedések megértésére, átfogóbb és mélyebb kutatásra lenne szükség, ami a social engineering pszichológiai vetületeit tárhatná fel az emberi viselkedés szempontjából. [61] [62]

Úgy gondolom ahhoz, hogy a csoporton belül csökkenteni tudjuk a támadások fenyegetettségét, a lehető legpontosabb képet kell kapjunk arról, mivel tudjuk felkészíteni, és megóvni e korcsoport tagjait az online térben. Így fontos lenne annak a vizsgálata is, hogy egyéb, és a dolgozatomban megfogalmazott technikai megoldások, különböző programok, kampányok, felhívások, milyen mértékben hasznosak, mennyire képesek növelni a biztonságra való törekvést, elkerülni a veszélyeket.

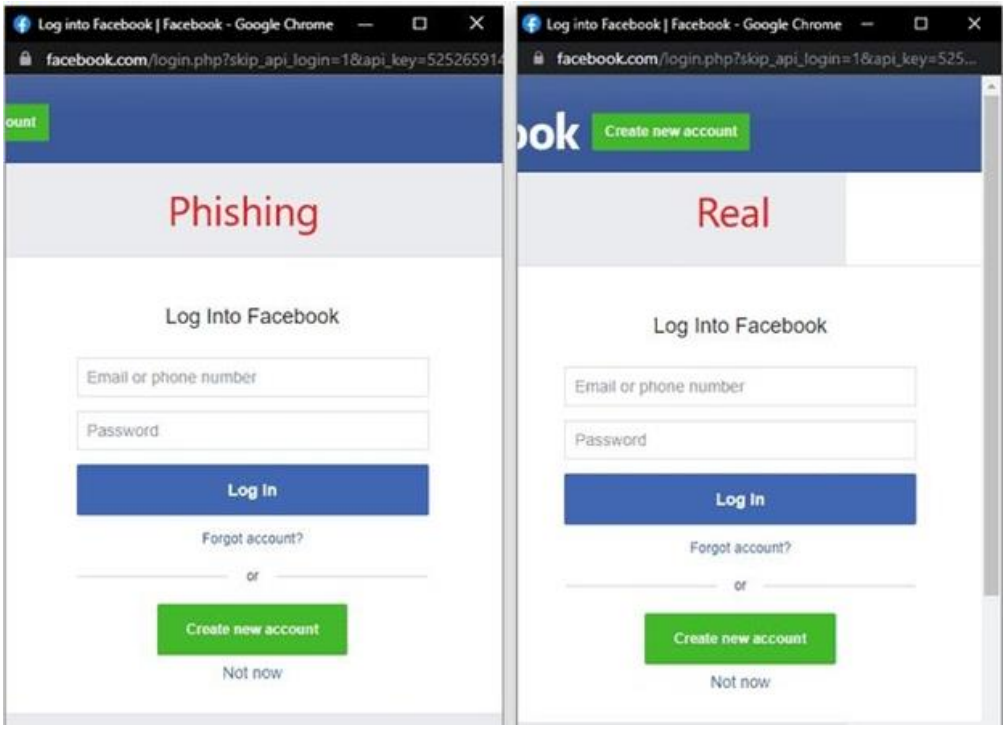
6.1 Áldozattá válás kockázatának csökkentése

A fejezetben röviden, és egyszerűen szeretném összefoglalni, a kutatásom második részére visszautalva, így elsősorban adathalász támadások esetében, hogy mit tehetünk annak érdekében, hogy csökkentsük, az áldozattá válás kockázatát.

Mindenekelőtt az internetezésre használt eszközön a legutolsó, rendszeres időközönként frissített operációs rendszer fusson. Rendelkezzünk vírusvédelmi, szintén rendszeresen

frissített programmal gépünkön. Ahol lehet használjuk a kétfaktoros hitelesítést. Minden esetben legyünk elővigyázatosak, mindig keressük az árulkodó jeleket. Ismeretlen e-mail esetén ha tudjuk ellenőrizzük a feladót hitelességét, csak olyan csatolmányt töltsünk le amiről tudjuk, hogy megbízható, fokozott óvatossággal kezeljük a hivatkozásokat, amennyiben nem vagyunk biztosak benne ne nyissuk meg a hivatkozásokat, ne töltsük le a csatolmányokat. Soha, sehol, semmilyen körülmények között ne adjuk meg jelszavainkat, személyes, és bankkártya adatainkat, semmilyen ügyfélszolgálat sem kérhet tőlünk ilyen adatokat. Keltsen bennünk gyanút ha sürgetnek, vagy azonnali cselekvésre sarkalnak, inkább álljunk meg, tartsunk szünetet, és mielőtt cselekszünk alaposan gondoljuk át. E-mail-ben figyeljünk a nyelvtani hibákat, nyelvhelyességet, magyartalan megfogalmazásokat, mely szintén erős jele lehet az adathalász támadásnak. Kezeljük kellő óvatossággal az általános üdvözlésekkel kezdődő leveleket. Az email tárgyát is minden esetben ellenőrizzük, valamint az aktualitását (rendeltem-e ilyen csomagot, tényleg nem fizettem be azt a számlát). Alaposan nézzük meg a feladó email címét, még akkor is ha látszólag megegyezik a jól ismert címről érkezőkkel, akár egy betű szándékos elírása, kihagyása is utal a csalók trükkjeire. Kövessük figyelemmel a médiában megjelenő adathalászattal kapcsolatos tájékoztatásokat. Nem szolgáltat kellő bizonyítékkal, de ellenőrizzük a webhelyek tanúsítványait is. Ne telepítsünk eszközeinkre olyan programot amit nem ismerünk. A böngésző címsávban különösen kritikus oldalak esetén, pl.: banki belépés, mindig alaposan nézzük meg a honlap címet, valóban az ismert címre lépünk-e be. [63] [64] [65] [66]

Fontos azonban leszögeznem, hogy szükséges az állandó figyelem, mert soha nem lehetünk elég óvatosak, és a veszélyek ellen felvértezettek, amit mi sem bizonyít jobban mint a legújabb adathalász technikák megjelenése. Manapság olyan módszert fejlesztettek ki, különböző kódolási trükkökkel, amivel az eredetivel mindenben megegyezőek oldalakat tudnak létrehozni. Az eljárást „Browser in the Browser”-nek nevezték el, mely eljárás kihasználja a weboldalak, harmadik féltől származó bejelentkezési alternatíváit (pl.: Google vagy Facebook fiókkal) felugró ablakokban, ahol egy böngészőablakot szimulálnak a böngészőn belül. Rendkívül megnehezíti a védekezést, hogy az URL-ek is teljesen azonosan lemásolásra kerülnek, mint ahogy azt a 6-3. ábra is mutatja. A módszer „még csak” Chrome böngészővel kompatibilis. [67] [68]



6-3. ábra: Browser in the Browser támadás [68]

A fejezettel célom volt irányvonalat mutatni azon személyeknek is, akik valami oknál fogva elolvassák munkámat és esetleg a vizsgált korcsoporthoz tartoznak, nem ismerve a veszélyek elkerülésének bevett, működő módszereit.

7 ÖSSZEGZÉS

Szakdolgozatommal saját közeli, és tágabb környezetemből is kiindulva, személyes tapasztalatok, valamint statisztikai meglátások alapján, szerettem volna bemutatni, és felmérni az idősebb generáció folyamatosan növekvő internet penetrációjához kapcsolódóan biztonságtudatosságukat, valamint ismereteiket a kibertérben lévő veszélyekről. Munkámban a témaválasztással kapcsolatban hipotéziseket is megfogalmaztam. Annak érdekében, hogy megismerhessük e veszélyeket, a második fejezetben a social engineering, vagyis a pszichológiai manipuláció fogalmának meghatározásával, és kérdéskörével foglalkoztam. Bemutatva különböző változatait, két nagy, a humán és számítógép alapú technikákra osztva a támadások fajtáit. Majd érintettem biztonság szempontjából a támadások sikerességét befolyásoló emberi tényezőket, melyeket a támadók könnyen ki tudnak használni. A dolgozat következő fejezeteiben elsősorban az adathalász technikákra helyeztem a hangsúlyt, tekintve, hogy a vizsgált korcsoport a mindennapokban ezen támadásokkal találkozhat legnagyobb számban, és a legnagyobb veszélyt is e támadási fajta jelentheti számukra. Dolgozatom következő részében kutatásomat mutattam be, mely két részből álló kérdőíves felmérést jelentett. Első részben a csoport digitális ismereteit mértem fel, majd a kérdőív gyakorlati, második felében 12 különböző valódi, vagy csaló levelek közül kellet választaniuk a kitöltőknek, opcionálisan indokolva válaszuk okát is. A jogszerűtlen, vagy legitim adathalász levelek kiválasztása a nem tudom válasz lehetőséggel, lehetővé tette a felmérésben részt vevők között a pszichológiai befolyásolás mélyebb megismerését. Annak érdekében, hogy a felmerült problémákról minél pontosabb képet kapjunk, így az esetleges korrelációk megállapítására, illetőleg a legpontosabb következtetések levonása érdekében, a kérdőívem átkódolásával, kereszttáblás statisztikai próbákat végeztem. Kiértékelésem alapján megállapítottam, hogy a korosztály erősen kitett a kiberbiztonsági veszélyeknek, ismerik és találkoztak is rosszindulatú támadással. Egyértelműen megállapítható, hogy fontos lenne körükben a biztonságtudatosságuk növelése, ezzel kapcsolatos kompetenciájuk bővítése, melyre egyértelmű igény is lenne csoportjukban. Azonban arra nem kaptam egyértelmű választ, pontosan milyen mértéket képvisel biztonságtudatosságuk, milyen mértékben felkészültek az internet jelentette veszélyekre, ezt további kutatás tárgyát képezhetné. Felmérésből a következtetéseket levonva, és leíró statisztika alapján, nem vagy csak részben igazoltam dolgozatom elején felvetett hipotéziseimet. Ezt követően e kutatás alapján próbáltam megoldásokat találni, javaslatokat tenni a védekezési lehetőségekre, valamint a veszélyek, és az áldozattá válás csökkentésére. Tanulmányok alapján új megvilágításba helyeztem az emberi tényező jelentőségét a támadások sikerességében. Mindent összevetve a digitalizáció egyre nagyobb térnyerésével, társadalmi szinten is kiemelten fontos lenne foglalkozni az idős korosztály internet penetrációjának folyamatos növekedésével, és az ebből fakadó veszélyekkel, következményekkel.

7.1 Summary

In my dissertation based on my personal experiences and statistical insights, I will present and assess the security awareness and knowledge of the older generation about the dangers in cyberspace, in relation to the ever increasing internet penetration. In my work, I have also formulated hypotheses related to the choice of topic. In order to understand these threats, in the second chapter, I have defined the concept of social engineering, a form of psychological manipulation, and dealt with the issues related to it. I have presented its different variants, dividing the types of attacks into two categories, human and computer-based techniques. Then I touched on human factors that affect the success of attacks, which can be easily exploited by attackers. In the following chapters of the dissertation, I have focused on phishing techniques, given that the age group under study is the most likely to encounter these attacks in their daily lives and the most threatening to them. In the next part of my thesis I presented my research, which consisted of a questionnaire survey in two parts. In the first part, I measured the digital knowledge of the group, and in the second part of the practical questionnaire, they were asked to choose between 12 different legitimate or illegitimate emails, with an optional explanation of the reason for their response. Choosing either illegitimate or legitimate phishing emails with the „I don't know" answer option allowed for a deeper understanding of psychological influence among the survey participants. In order to get as accurate a picture as possible of the problems encountered, in order to establish possible correlations and to draw the most accurate conclusions, I performed cross-tabular statistical tests by recoding my questionnaire. Based on my evaluation, I found that the age group is heavily exposed to cybersecurity threats, they know a malicious attack and have encountered too. It is clear that it would be important to increase their security awareness and competenc, and there is a clear need for this in their group. However, I did not get a clear answer as to what exactly is the extent of their security awareness and to what extent are they prepared for the dangers of the Internet, which could be the subject of further research. Drawing conclusions from the survey and using descriptive statistics, I have not or only partially confirmed the hypotheses I put forward at the beginning of my thesis. Subsequently, on the basis of this research, I have tried to find solutions and make suggestions on ways to protect against and reduce the risks and victimisation. Based on studies, I have shed new light on the importance of the human factor in the success of attacks. All in all, with the increasing prevalence of digitalisation, it would be especially important to address the continuous increase of the Internet penetration of the elderly and the resulting dangers and consequences on the social level as well.

8 ÁBRAJEGYZÉK

9 IRODALOMJEGYZÉK

[1] Kollár, Cs., Zakar, Á.: A social engineering és a manipulációs technikák és módszerek. *Biztonságtudományi Szemle*, Vol. 2., No. 2., 2020, 23-38. old. (https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/58/50), utoljára megtekintve: 2021. 04. 08.

[2] (https://www.ksh.hu/docs/hun/xftp/idoszaki/tavkint/20213/tavkozles_21_3.pdf), utoljára megtekintve: 2022. 02. 04.

[3] (https://www.ksh.hu/stadat_files/ikt/hu/ikt0029.html), utoljára megtekintve: 2022. 02. 04.

[4] Az információbiztonság lélektana. KÖFOP-2.2.2-VEKOP-16-2016-00001tanulmány (https://nki.gov.hu/wp-content/uploads/2019/07/01-Az-inform%C3%A1ci%C3%B3biztons%C3%A1g-l%C3%A9lektana.pdf), utoljára megtekintve: 2021. 04. 12.

[5] Nyikes, Z.: Az információbiztonság növelése a felhasználó támogatásának lehetőségeivel. Óbudai Egyetem, Doktori (PhD) értekezés Budapest, 2018.

[6] Kollár, Cs., Zakar, Á.: A social engineering és a manipulációs technikák és módszerek-Kutatási jelentés. *Biztonságtudományi Szemle*, Vol. 2., No. 3., 2020, 31-46. old. (https://biztonsagtudomanyi.szemle.uniobuda.hu/index.php/home/article/view/70/62), utoljára megtekintve: 2021. 04. 08.

[7] Oroszi, E.: Social engineering – Az emberi erőforrás, mint az információbiztonság kritikus tényezője, Budapest: Corvinus Egyetem, 2008. (http://docplayer.hu/3827943-Social-engineering-az-emberi-eroforras-mint-az-informaciobiztonsag-kritikus-tenyezoje.html), utoljára megtekintve: 2021. 04. 16.

[8] Karakasiliotis, A., Furnell, S., M., Papadaki, M.: Assessing end-user awareness of social engineering and phishing, (https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1011&context=isw), utoljára megtekintve: 2021.04.19.

[9] Maqousi, A., Balikhina, T., Mackay, M.: An effective method for information security awareness raising initiatives, *IJCSIT* Vol 5, No. 2, 2013, pp. 63-72 (http://www.airccse.org/journal/jcsit/5213ijcsit06.pdf), utoljára megtekintve: 2021.05.02.

[10] Tarján, G.: Az információbiztonsági tudatosság érettségi szintjének mérése szervezetekben. Budapest Corvinus Egyetem, Doktori értekezés Budapest, 2020. (http://phd.lib.uni-corvinus.hu/1090/1/Tarjan_Gabor_dhu.pdf), utoljára megtekintve: 2021.05.02.

[11] Som, Z.: Kibertudatosság különböző színtereken. Nemzeti Közszolgálati Egyetem, Doktori (PhD) értekezés Budapest, 2021. (https://antk.uni-nke.hu/document/akk-copy-uni-nke-hu/Som%20Zolt%C3%A1n%20disszert%C3%A1ci%C3%B3tervezet.pdf) utoljára megtekintve: 2022.01.14.

[12] Mitnick, Kevin D.: A legendás hacker. A rábeszélés művészete. *Perfact-Pro*, 2003.

[13] Deák, V.: A social engineering humán alapú támadási technikái, (https://biztonsagpolitika.hu/wp-content/uploads/2017/04/Deak_Veronika_a-social-engineering-hum%C3%A1n-alap%C3%BA-t%C3%A1mad%C3%A1si-technik%C3%A1i.pdf), utoljára megtekintve: 2021. 04. 21.

[14] Bányász, P.: Social engineering and social media. *Nemzetbiztonsági Szemle*, VI. évfolyam, 1. szám, 2018, 59-77. old. (http://real.mtak.hu/94335/1/EPA02538_nemzetbiztonsagi_szemle_2018_01_059-077.pdf), utoljára megtekintve: 2021. 04. 20.

[15] Reynolds, V.: Social Engineering. The Art of Psychological Warfare, Human Hacking, Persuasion, and Deception. *CreateSpace Independent Publishing Platform*, 2016

[16] Oroszi, E.: Social engineering támadási technikák. Avagy a végső megoldás: a felhasználó, (https://www.securinfo.hu/termekek/it-biztonsag/1295-social-engineering-tamadasi-technikak- avagy-a-vegso-megoldas-a-felhasznalo.html), utoljára megtekintve: 2021.04.23

[17] Walker, L. E.: Deception of Phishing: Studying the Techniques of Social Engineering by Analyzing Modern-day Phishing Attacks on Universities, (https://etd.auburn.edu/bitstream/handle/10415/5175/LEW%20Thesis.pdf?sequence=&isAllowed=y), utoljára megtekintve: 2021. 04. 19.

[18] Breda, F., Barbosa, H., Morais, T.: SOCIAL ENGINEERING AND CYBER SECURITY, (https://www.researchgate.net/profile/Hugo-Barbosa/publication/315351300_SOCIAL_ENGINEERING_AND_CYBER_SECURITY/links/599c43430f7e9b892bafc0df/SOCIAL-ENGINEERING-AND-CYBER-SECURITY.pdf?origin=publication_detail), utoljára megtekintve: 2021. 04. 23.

[19] Salahdine, F., Kaabouch, N.: Social Engineering Attacks: A Survey, (https://www.mdpi.com/1999-5903/11/4/89/htm), utoljára megtekintve: 2021. 04. 23.

[20] Thapar, A.: Social Engineering - An attack vector most intricate to tackle, (http://www.infosecwriters.com/text_resources/pdf/Social_Engineering_AThapar.pdf), utoljára megtekintve: 2021. 04. 23.

[21] Hadnagy, Ch.: Social Engineering The Art of Human Hacking. *Wiley Publishing*, 2011.

[22] Hadnagy, Ch: Social Engineering The Science of Human Hacking. *John Wiley & Sons, Inc*., 2018.

[23] Watson, G., Mason, A., Ackroyd, R.: Social Engineering Penetration Testing. Executing Social Engineering Pen Tests, Assessments and Defense. *Elsevier*, 2014.

[24] Koyun, A., AI Janab, E.: Social Engineering Attacks, (https://www.jmest.org/wp-content/uploads/JMESTN42352270.pdf), utoljára megtekintve: 2021.04. 26.

[25] Marino, M.: The 20 Most Hacked Passwords in the World: Is Yours Here? (https://www.safetydetectives.com/blog/the-most-hacked-passwords-in-the-world/), utoljára megtekintve: 2021.05.12.

[26] Vass, E.: Nem erős, de legalább gyenge, Ez a tipikus magyar jelszó! (https://www.itbusiness.hu/technology/aktualis_lapszam/tech/Ez_a_tipikus_magyar_jelszo), utoljára megtekintve: 2021. 05. 12.

[27] Deák, V.: Social engineering alapú információszerzés a kibertérben megvalósuló lélektani műveletek során, (https://core.ac.uk/download/pdf/275587983.pdf), utoljára megtekintve: 2021.04. 26.

[28] Akshat Jain, Harshita Tailang, Harsh Goswami, Soumiya Dutta, Mahipal Singh Sankhla, Rajeev Kumar: Social Engineering: Hacking a Human Being through Technology, (https://www.researchgate.net/publication/309234725_Social_Engineering_Hacking_a_Human_Being_through_Technology), utoljára megtekintve: 2021. 04. 28

[29] Kontio, M.: Social Engineering 101. Bachelor's thesis, Turku University Of Applied Sciences Business Information Technology, Business Data Communications and Information Security 2016. (https://core.ac.uk/download/pdf/38134896.pdf), utoljára megtekintve: 2021. 05. 11

[30] Social engineering vagyis a pszichológiai manipuláció, (https://maxer.hu/blog/social-engineering-vagyis-a-pszichologiai-manipulacio/), utoljára megtekintve: 2021. 04. 28

[31] Fischer TH., A., Tóth G.: Az internet csapdái-így védje magát! *CHIP*, 2021/03 72-77. old.

[32](https://www.otpbank.hu/static/portal/sw/pic/Adathalasz_kiserlet_20190806_2048.jpg) utoljára megtekintve: 2021.03.17.

[33] Patel, S. R.: Kali Linux Social Engineering *Packt Publishing Ltd*, 2013.

[34] What is Typosquatting? – Definition and Explanation, (https://www.kaspersky.com/resource-center/definitions/what-is-typosquatting), utoljára megtekintve: 2022. 02. 03.

[35] IT café: Céges biztonság: az első számú kockázat az alkalmazott. (https://itcafe.hu/hir/symantec_jelentes_vallalati_biztonsag.html), utoljára megtekintve: 2021. 05. 12.

[36] Oriyano, P., S.: CEH v9 Certified Ethical Hacker Version 9 Study Guide, *Sybex,* 2016.

[37] Bisson, D.: 5 Social Engineering Attacks to Watch Out For, (https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/), utoljára megtekintve: 2021. 04. 28.

[38] Leitold, F.: Sebezhetőségvizsgálatok a gyakorlatban, NKE, Budapest, 2014. (http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/10450/Teljes%20sz%C3%B6veg%21?sequence=1&isAllowed=y), utoljára megtekintve: 2021. 04. 21.

[39] (https://nki.gov.hu/it-biztonsag/tanacsok/kiberbiztonsagi-kerdoiv-a biztonsagtudatossag-jegyeben/), utoljára megtekintve: 2021. 10. 14.

[40] Hilóczki, M.: Jelszóhasználati szokások empirikus elemzése, Miskolci Egyetem, 2016. (http://midra.uni-miskolc.hu/document/24160/18984.pdf), utoljára megtekintve: 2021.10. 14.

[41] Rosenthal, M.: Must-Know Phishing Statistics: Updated 2021 (https://www.tessian.com/blog/phishing-statistics-2020/), utoljára megtekintve: 2022. 02. 27.

[42] APWG: Phishing Activity Trends Reports (https://apwg.org/trendsreports/), utoljára megtekintve: 2022.02.27.

[43] APWG: Phishing Activity Trends Report, 4th Quarter 2020 (https://docs.apwg.org//reports/apwg_trends_report_q4_2020.pdf), utoljára megtekintve: 2022. 02. 27.

[44] Dub, M., Bányász, P.: Do not feed the phish! (https://www.ludovika.hu/blogok/cyberblog/2021/04/29/do-not-feed-the-phish/), utoljára megtekintve: 2022.02.27.

[45] NetUtils: Social Engineering. Is the Worst Yet to Come? (https://netutilsblog.com/tag/javvad-malik/), utoljára megtekintve: 2022. 02. 27.

[46] Sara Pan: FBI's IC3 Report: Financial Losses Due to Email Fraud Hit Record High in 2021, (https://www.proofpoint.com/us/blog/email-and-cloud-threats/fbis-ic3-report-financial-losses-due-email-fraud-hit-record-high-2021), utoljára megtekintve: 2022.04.02.

[47] 2021 IC3 Internet Crime Report Released by FBI, (https://cyberconiq.com/news/2021-ic3-internet-crime-report-released-by-fbi/), utoljára megtekintve: 2022. 04 .02.

[48] FEDERAL BUREAU of INVESTIGATION Internet Crime Riport 2021, (https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf), utoljára megtekintve: 2022. 04. 02.

[49] Németh, A.: Adatelemzés statisztikai módszerekkel. (http://eta.bibl.u-szeged.hu/458/1/EFOP343_AP2ETSZK_jegyzet_N%C3%A9meth_Anik%C3%B3_Adatelemz%C3%A9s_statisztikai_m%C3%B3dszerekkel_20180620.pdf), utoljára megtekintve: 2022. 04. 30

[50] Lengyelné Molnár T.: On-line értékelési módszerek II. (https://dtk.tankonyvtar.hu/xmlui/bitstream/handle/123456789/12458/06_on-line_ertekelesi_modszerek_ii.pdf?sequence=1&isAllowed=y), utoljára megtekintve: 2022. 04. 30

[51] Mayer, A.: SPSSABC.HU, (https://spssabc.hu/ketvaltozos-elemzes/khi-negyzet-proba/), utoljára megtekintve: 2022. 04. 30

[52] Knoke, F., Bényi L.: A jelszó új alternatívája? *CHIP*, 2021/02 16-19. old

[53] Hlács, F.: FIDO2 támogatást kap az Android, webre is jön a biometrikus beléptetés (https://www.hwsw.hu/hirek/60043/fido2-google-fido-alliance-biztonsag.html), utoljára megtekintve: 2022. 04. 02.

[54] BITPORT: Nagy lépés az Androidnál a jelszavak nyugdíjazására (https://bitport.hu/nagy-lepes-az-androidnal-a-jelszavak-nyugdijazasara), utoljára megtekintve: 2022. 04. 02.

[55] NKI, IT Biztonsági hírek, (https://nki.gov.hu/it-biztonsag/hirek/a-google-az-apple-es-a-microsoft-tett-egy-komoly-lepest-a-jelszomentes-jovo-fele/) utoljára megtekintve: 2022. 05. 09.

[56] Areej Alhogail; Afrah Alsabih.: Applying machine learning and natural language processing to detect phishing email, (https://www.sciencedirect.com/science/article/pii/S0167404821002388?via%3Dihub), utoljára megtekintve: 2021. 12. 17.

[57] Natural language processing (NLP) explained, (https://www.egress.com/resources/cybersecurity-information/phishing/natural-language-processing-nlp-explained), utoljára megtekintve: 2022. 05. 09.

[58] Thorpe, J: Schwartz, S.: Using Machine Learning To Identify Phishing Attacks, (https://assets.ctfassets.net/kdr3qnns3kvk/5VuciSuo36Ac2eeyU02ywE/941f363e586c71cda688aca307b851fd/Thorpe-PACISE2017.pdf), utoljára megtekintve: 2022. 05. 09.

[59] HVG: A Google csinált egy programot, amivel jelentheti a gyanús weboldalakat, (https://hvg.hu/tudomany/2019061_google_chrome_bovitmeny_gyanus_weboldal_jelentese), utoljára megtekintve: 2022. 04. 11.

[60] NKI: Pszichológiai befolyásolás–védekezés a csalások ellen, (https://nki.gov.hu/wp-content/uploads/2019/03/21_Pszichologiai-befolyasolas-vedekezes-a-csalasok-ellen.pdf), utoljára megtekintve: 2022. 04. 25.

[61] Coroneos, P.: Is cyber risk behaviour neurologically based? (https://www.linkedin.com/pulse/cyber-risk-behaviour-neurologically-based-peter-coroneos), utoljára megtekintve: 2021. 12. 17.

[62] Dömös, Zs.: Az agyunk is felelős azért, hogy nem vagyunk elég óvatosak az interneten, (https://24.hu/tech/2021/10/02/peter-coroneos-itbn-emberi-agy-evolucio-kiberfenyegetes-kiberbiztonsag-tamadas-social-engineering/) utoljára megtekintve: 2021. 12. 17.

[63] ESET: Az Adathalászat felismerése és védekezés ellene, (https://www.eset.com/hu/adathalaszat/), utoljára megtekintve: 2022. 04. 20.

[64] OTP Bank: Figyelemfelhívás, (https://www.otpbank.hu/portal/hu/Adathalaszat), utoljára megtekintve: 2021. 12. 17.

[65] Microsoft: Adathalászat elleni védelem, (https://support.microsoft.com/hu-hu/windows/adathal%C3%A1szat-elleni-v%C3%A9delem-0c7ea947-ba98-3bd9-7184-430e1f860a44) utoljára megtekintve: 2021. 12. 17.

[66] Gray, T.: 4 hatékony módszer a Phising támadások ellen, (https://www.websupport.hu/blog/2021/04/4-hatekony-modszer-a-phising-tamadasok-ellen/), utoljára megtekintve: 2022. 12. 17.

[67] Vaas, L.: Browser-in-the-Browser Attack Makes Phishing Nearly Invisible, (https://threatpost.com/browser-in-the-browser-attack-makes-phishing-nearly-invisible/179014/), utoljára megtekintve: 2022. 03. 24.

[68] HVG: Jól nézze meg: ha ilyen ablak ugrik fel a Chrome-ban, akkor épp lopni akarnak öntől, (https://hvg.hu/tudomany/20220329_adatlopas_adatvedelem_adathalaszat_mr_d0x_chrome_kamu_ablak?fbclid=IwAR1-tCg4gFYzHoZhgVCoaS5yTrvjDAYfG7hPYsBaB-IezTS4slku_-HuQqQ), utoljára megtekintve: 2022. 03. 24.

10 MELLÉKLETEK

Kérdőív
(a kérdőívben szereplő levelek saját forrás, ahol nem, ott jelölve a forrás.)

*A kérdőív második részében az e-mail üzenetek kiválasztásánál, csak az első levélnél tüntettem fel válasz lehetőségeket, tekintettel, hogy azok minden e-mail-nél megegyeznek.

Kiberbiztonsági kérdőív

Kedves Hölgyem/Uram!

Szabó Árpád vagyok az Óbudai Egyetem Neumann János Informatikai Kar Kiberbiztonsági szak hallgatója. Szakdolgozatomat a biztonságtudatosság és az ehhez kapcsolódó social engineering, vagyis a pszichológia manipuláción, megtévesztésen alapuló hacker támadási technikákról írom, az idősebb internethasználók körében. Ehhez kérném az Ön segítségét a lenti kérdőív kitöltésével, amennyiben elmúlt 55 éves és rendszeresen használ internetet.

A kérdőív kitöltése anonim módon zajlik, az adatok kizárólag a szakdolgozatomban jelennek meg, kiértékelése összesítve történik, egyéni információk nem azonosíthatóak.

A kérdőív kitöltése körülbelül 20 percet vesz igénybe, és 2022. február 25-ig tölthető ki.
Ahol egyszerre több válasz is adható azt külön feltüntetésre került.

A kérdőív két részből áll, az első rész rövid feleletválasztós kérdéseket tartalmaz, a másik felében pedig e-mail levelekről kell eldönteni, hogy azok valós, vagy csaló levelek lehetnek, rövid indoklással ellátva.

Amennyiben kérdése merülne fel a kérdőívvel kapcsolatban, kérem lépjen kapcsolatba velem az arpads.oe@gmail.com e-mail címen.

Segítő együttműködését előre is köszönöm!

Neme *

- férfi
- nő

Kora (év) *

Rövid szöveges válasz

Lakóhelye *

- főváros
- nagyváros, megyeszékhely
- kisváros
- község, falu
- tanya

Legmagasabb iskolai végzettsége *

- kevesebb, mint 8 osztály
- befejezett 8 osztály
- szakmunkásképző
- OKJ-s vagy technikusi végzettség
- gimnáziumi érettségi
- szakközépiskolai érettségi
- főiskolai v. egyetemi diploma

Milyen területen dolgozik, dolgozott? (Több választ is megjelölhet) *

- [ ] adminisztráció
- [ ] bank
- [ ] egészségügy
- [ ] értékesítés, kereskedelem
- [ ] gyártás, termelés
- [ ] humán erőforrás
- [ ] informatika
- [ ] telekommunikáció
- [ ] marketing, média
- [ ] jog
- [ ] közigazgatás
- [ ] mérnök, műszaki
- [ ] oktatás
- [ ] pénzügy, számvitel
- [ ] ügyfélszolgálat, recepció
- [ ] vendéglátás, idegenforgalom
- [ ] cégvezetés, menedzsment
- [ ] Egyéb...

Milyen informatikai eszközzel rendelkezik? (Több választ is megjelölhet) *

- [ ] számítógép
- [ ] laptop
- [ ] tablet
- [ ] okostelefon
- [ ] okosóra
- [ ] okoskarkötő
- [ ] okos háztartási és egyéb okos eszközök (pl.: hűtő, TV stb.)
- [ ] Egyéb...

Milyen eszközön, eszközökön szokott a leggyakrabban internetezni? (Több választ is megjelölhet) *

- [ ] asztali számítógép
- [ ] laptop
- [ ] tablet
- [ ] mobiltelefon
- [ ] Egyéb...

Milyen gyakran használja az internetet? *

- ( ) csak különleges alkalmakkor
- ( ) évente párszor
- ( ) havonta többször
- ( ) hetente többször
- ( ) naponta
- ( ) folyamatosan használja az internetet

Milyen tevékenységet végez az interneten? (Több választ is megjelölhet) *

- [ ] hírek, cikkek olvasása
- [ ] szakcikkek olvasása
- [ ] információ keresése
- [ ] navigáció, tájékozódás (pl.: Google Maps, Waze)
- [ ] e-mail-ek küldése, fogadása.
- [ ] internetes telefonálás (pl.: Skype, Viber, Messenger stb.).
- [ ] chat-elés (pl.: Skype, Viber, Messenger stb.).
- [ ] közösségi oldalon olvasás, posztolás (pl.: Facebook, Twitter, Instagram).
- [ ] társkereső oldalak használata
- [ ] 18+ tartalmak megtekintése
- [ ] torrentezés
- [ ] filmnézés (pl. YouTube, Netflix)
- [ ] játék
- [ ] zenehallgatás (pl.: YouTube, Spotify)
- [ ] sportfogadás, szerencsejáték
- [ ] internetes vásárlás/eladás (pl.: eBay, Vatera, Jófogás)
- [ ] tanulás (pl.: DuoLingo)
- [ ] ügyintézés (pl.: Ügyfélkapu)
- [ ] internetes bankolás
- [ ] online vásárlás (pl.: élelmiszer, bútor, divatáru, elektronika stb.)
- [ ] podcast hallgatás
- [ ] különböző tematikus csatornák (pl.: YouTube-on) megtekintése
- [ ] Egyéb...

Ön szerint mennyire ért az internethez? *

- ◯ nem értek hozzá
- ◯ kicsit értek hozzá
- ◯ felhasználói szinten
- ◯ az átlagos felhasználóktól jobban
- ◯ professzionális szinten

Ön szerint melyik online szolgáltatás tárol Önről adatokat? (Több választ is megjelölhet) *

- ☐ közösségi oldalak (Facebook, Instagram, TikTok, stb.)
- ☐ e-mail szolgáltatók (gmail.com, freemail.hu, citromail.hu, stb.)
- ☐ kereső-motorok (Google, Yahoo, Bing, stb.)
- ☐ nem tudom

Kérem, fejezze be a mondatot! Zsarolóvírusnak nevezzük azokat a rosszindulatú programokat, amelyek... *

- ◯ titkosítják a számítógépes eszközön tárolt adatokat
- ◯ ellopják a felhasználók jelszavait
- ◯ nem tudom

Használ-e bármilyen védelmi programot (pl.: vírusirtó) eszközein melyeken internetezik? *

- ◯ igen, ingyenes verziót
- ◯ igen, fizetős verziót
- ◯ nem
- ◯ nem tudom
- ◯ Egyéb...

Fontosnak tartja-e, hogy legyen védelmi szoftver eszközein? *

- ○ nagyon fontosnak
- ○ kevésbé fontosnak
- ○ nem különösebben
- ○ egyáltalán nem

Amennyiben rendelkezik vírusirtó programmal rendszeresen frissíti-e?

- ○ igen
- ○ nem foglalkozom a frissítéssel
- ○ szükség esetén
- ○ magától frissül a vírusírtó program
- ○ nem tudom
- ○ Egyéb...

Hány karakter hosszú a leghosszabb jelszava? *

- ○ 1-5 között
- ○ 5-10 között
- ○ 10-15 között
- ○ 15-20 között
- ○ 20 felett

Milyen karakterkombinációjú jelszót használ? (Több választ is megjelölhet) *

- ☐ van benne kisbetű
- ☐ van benne nagybetű
- ☐ van benne szám
- ☐ van benne speciális karakter (pl.: _ alsóvonal)

Milyen gyakran változtatja meg jelszavát? *

- ○ naponta
- ○ hetente
- ○ havonta
- ○ negyed évente
- ○ évente
- ○ ritkábban, mint évente
- ○ nem szokta megváltoztatni
- ○ csak ha szükséges
- ○ amikor eszébe jut
- ○ minden gyanús körülmény esetén
- ○ amikor a felület/alkalmazás kéri
- ○ Egyéb...

Használja ugyanazt a jelszót több helyen is? *

- ○ igen
- ○ nem

Hogyan jegyzi meg a jelszavát, hol tárolja őket? (Több választ is megjelölhet) *

- ☐ megtanulom, fejben tartom
- ☐ feljegyzem a telefonomba
- ☐ jelszókezelő szoftver használok
- ☐ ha mód van a lementésére, akkor úgy eltárolom
- ☐ felírom egy cetlire, füzetbe stb.
- ☐ Egyéb...

Van-e olyan jelszava, amelyet más is tud? *

- igen
- nem
- nem válaszolok

Előfordult Önnel, hogy kiadta a jelszavát? *

- igen
- nem

Amennyiben az előző válaszra igennel válaszolt, kérem, röviden írja le az esetet

Hosszú szöveges válasz

Jelszóválasztásnál legfontosabb, hogy a jelszavam *

- legyen könnyen megjegyezhető
- legyen biztonságos
- mindkettő

Milyen gyakorisággal szokott adatmentést készíteni eszközéről/eszközeiről? *

- naponta
- hetente
- havonta
- félévente
- legalább évente
- ritkábban
- csak bizonyos adatokról szoktam rendszertelenül (pl.: családi fotók)
- nem szoktam adatmentést készíteni
- Egyéb...

Milyen jellegű adatokat tárol okostelefonján? (Több választ is megjelölhet)

- [ ] címek
- [ ] e-mail címek
- [ ] naptárbejegyzések
- [ ] jelszavak
- [ ] személyes adatok (pl. bankszámlaszám, TAJ szám, adószám, stb.)
- [ ] személyes dokumentumok
- [ ] pénzügyi dokumentumok
- [ ] orvosi leletek
- [ ] munkahelyi dokumentumokat
- [ ] családi képek és videók
- [ ] bizonyítványok szkennelt változatát
- [ ] Egyéb...

Hogyan kezeli az e-mail üzenetekkel érkező mellékleteket, csatolmányokat? *

- ( ) soha nem nyitom meg, félek a vírusoktól
- ( ) csak az ismert címről érkező mellékelteket nyitom meg
- ( ) minden mellékletet, csatolmányt megnyitok
- ( ) a levél tartalmától függően megnyitja (pl.: számlabefizetéssel kapcsolatos értesítők, banki levelek, stb.)
- ( ) Egyéb...

Részt venne-e (online, ingyenes) informatikai biztonságtudatosságot növelő képzésen? *

- ◯ igen
- ◯ nem
- ◯ nem tudja
- ◯ vettem már részt ilyen képzésben

Mi okozza Önnek a legnagyobb nehézséget számítógépkezelés, internetezés alkalmával? *

Hosszú szöveges válasz

Milyen operációs rendszert használ számítógépén?

- ◯ Windows 7
- ◯ Windows 8
- ◯ Windows 10
- ◯ Windows 11
- ◯ a Windows 7-nél régebbi Windows operációs rendszert
- ◯ Linux
- ◯ Mac OS
- ◯ nem tudom
- ◯ Egyéb...

Rendszeres időközönként frissíti-e operációs rendszerét?

- ◯ igen
- ◯ nem
- ◯ be van állítva az automatikus frissítés
- ◯ nem tudom

Ön általában milyen adatvédelmi és biztonsági beállításokat alkalmaz okoseszközein (pl.: okostelefonján)? (Több választ is megjelölhet) *

- [ ] a gyári beállításokat, semmit nem módosítok
- [ ] képernyőzárat
- [ ] a nem használt funkciókat (pl.: helymeghatározás, Bluetooth, stb.) kikapcsolom
- [ ] felülvizsgálom a hozzáférési jogosultságokat, és letiltom azokat, amik nem szükségesek a működéshez
- [ ] nem tudom
- [ ] Egyéb...

Ön milyen gyakorisággal telepít biztonsági frissítést eszközein? *

- ( ) amint kijönnek a frissítések, mert be van állítva az automatikus frissítés
- ( ) amint kijönnek a frissítések, és van rá időm
- ( ) amikor már nem tudom rendesen használni az eszközt
- ( ) soha
- ( ) nem tudom
- ( ) Egyéb...

Otthoni routerén változtat-e az alapértelmezett beállításokon (pl.: WiFi jelszó) a biztonságért? * (Több választ is megjelölhet)

- [ ] igen, mindig
- [ ] csak ha szükséges
- [ ] soha
- [ ] nem tudom, hogyan kell megváltoztatni
- [ ] nem tudom, mit kellene megváltoztatni
- [ ] mi az a router?
- [ ] Egyéb...

Találkozott-e már vírusfertőzéssel, adathalász e-mailekkel és/vagy egyéb rosszindulatú támadással Ön, vagy esetleg ismerőse? *

- ◯ igen
- ◯ nem
- ◯ nem tud róla
- ◯ csak ismerős találkozott

Amennyiben találkozott már adathalász e-mailekkel, vírus-, és/vagy egyéb rosszindulatú támadással Ön, vagy esetleg ismerőse, ezután biztonságtudatosabb lett-e, jobban védi-e az eszközeit, jobban odafigyel-e a biztonságra?

- ◯ igen, azóta igyekszem figyelni rá
- ◯ csak az első pár napban
- ◯ nem tartottam szükségesnek
- ◯ Egyéb...

Előfordult már, hogy egy ismeretlen feladótól érkező elektronikus levél ajánlására látogatott meg egy weboldalt, töltött le valamit, rendelt meg valamit, vagy fizetett valamit? *

- ◯ igen
- ◯ nem

Használ-e kétfaktoros hitelesítést? *

- ◯ igen
- ◯ nem
- ◯ csak ahol szükséges
- ◯ nem tudom
- ◯ nem ismerem a kétfaktoros hitelesítést

Használ-e jelszómenedzser programot? *

- ○ igen
- ○ nem
- ○ nem tudom
- ○ nem ismerek ilyen programokat

Milyen közösségi oldalakat látogat, használ leggyakrabban? *

Hosszú szöveges válasz

A közösségi oldalakon milyen adatokat, információkat oszt meg? (Több választ is megjelölhet) *

- ☐ személyes adatok
- ☐ aktuális tartózkodási hely
- ☐ telefonszám
- ☐ családi állapot és családi kapcsolat
- ☐ családi, baráti képek
- ☐ munkahelyi képek
- ☐ képek földrajzi hely információval
- ☐ Egyéb...

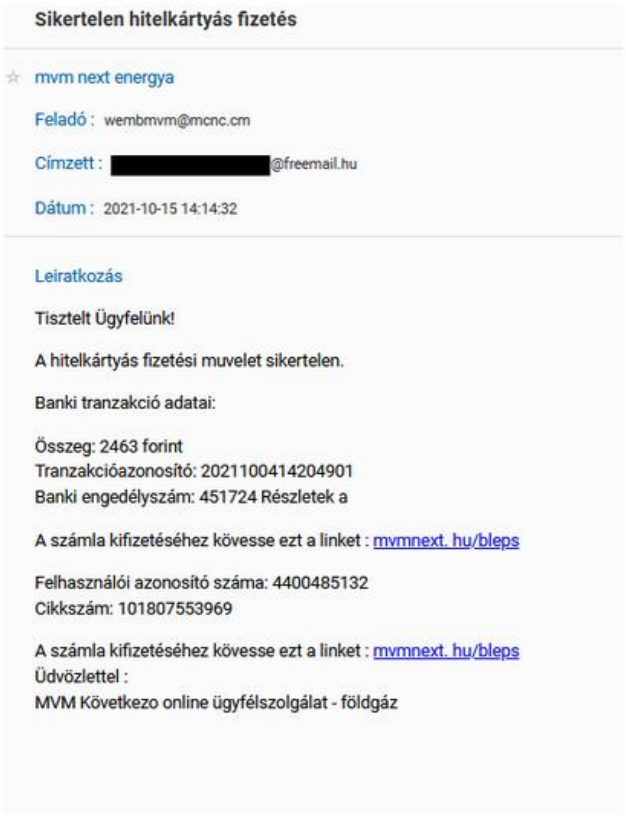
Nyilvános WiFi hálózaton (pl.: szálloda, kávézó, repülőtér) szokott-e internetezni saját eszközzel *

- ○ igen
- ○ nem
- ○ csak ha szükséges
- ○ Egyéb...

Nyilvános WiFi használat esetén milyen tevékenységeket szokott végezni az eszközein? (Több választ is megjelölhet)

- [ ] bejelentkezés online szolgáltatásokba (pl.: e-mail fiók ellenőrzése, netbank használata, közösségi média f ...
- [ ] böngészés hírportálokon
- [ ] dokumentumok, fájlok letöltése
- [ ] Egyéb...

1 Kérem ítélje meg a következő e-mail levél legitimitását *



Sikertelen hitelkártyás fizetés

☆ mvm next energya

Feladó : wembmvm@mcnc.cm

Címzett : [redacted]@freemail.hu

Dátum : 2021-10-15 14:14:32

Leiratkozás

Tisztelt Ügyfelünk!

A hitelkártyás fizetési muvelet sikertelen.

Banki tranzakció adatai:

Összeg: 2463 forint
Tranzakcióazonosító: 2021100414204901
Banki engedélyszám: 451724 Részletek a

A számla kifizetéséhez kövesse ezt a linket : mvmnext. hu/bleps

Felhasználói azonosító száma: 4400485132
Cikkszám: 101807553969

A számla kifizetéséhez kövesse ezt a linket : mvmnext. hu/bleps
Üdvözlettel :
MVM Következo online ügyfélszolgálat - földgáz

- ( ) valódi, legitim
- ( ) nem valódi, csaló
- ( ) nem tudom

Kérem röviden indokolja az előző kérdésre adott válaszát, hogy mi alapján döntött

Hosszú szöveges válasz

2 Kérem ítélje meg a következő e-mail levél legitimitását *

Ajándékozzon valódi élményeket szeretteinek ✈

repjegy.hu ✈

Feladó : hirlevel@repjegy.hu

Címzett : [redacted]@freemail.hu

Dátum : 2020-12-09 15:48:31

Leiratkozás

repjegy.hu

06 1 510 0550

H-P: 10:00 - 18:00

Kedves [redacted]d!

A karácsonyi ajándék beszerzése sosem egyszerű feladat! A tavaly kapott nyakkendő azóta is a szekrény belsejében pihen, de a fülbevaló is csak egyszer került elő az ajándékdobozából!

A tökéletes ajándék!

Egy repülős utazásnál nem is lehetne szebb ajándékot találni, hiszen az utazás élménye örök! Tegyen Ön is repjegy utalványt a fa alá, és várja együtt szeretteivel, hogy a járvány után újra részese lehessen a világ felfedezésének!

Repjegy utalvány

Ajándékozzon egy felejthetetlen élményt szeretteinek!

Úti céltól és légitársaságtól függetlenül, bármely repülőjegyre beváltható 1 éven keresztül.
Egyszerűen megvásárolható online, és bankkártyával illetve átutalással is fizethető.
Az utalvány értékét Ön választhatja ki, sőt még egy rövid, személyre szóló üzenetet is megadhat.
A megvásárolt utalványt azonnal, nyomtatható változatban is elküldjük, így kézzelfogható formában is átadhatja szeretteinek.

Repjegy utalványt szeretnék

3 Kérem ítélje meg a következő e-mail levél legitimitását *

Értesítő

Feladó : info@dm.targetmax.hu

Címzett : [redacted]freemail.hu

Dátum : 2021-06-16 14:56:37

Leiratkozás

KEDVES [redacted]d!

Nézze meg ki nyerte a PROAKTIVdirekt aktuális sorsolásán a pénzt, amit a virtuális számláján összegyűjtött! Ha már tag, csak jelentkezzen be és ezzel az új sorsoláson is részt vesz. Ha még nem regisztrált, most megtehetí! Válaszaival gyűjtsön akár több millió forintot, amit minden sorsoláson megnyerhet. Sőt, ha partnereink ingyenes játékain is résztvesz, további értékes ajándékokat is nyerhet!

MEGNÉZEM KI NYERT ÉS CSATLAKOZOM AZ ÚJ SORSOLÁSHOZ IS!

A játék teljesen díjmentes!

Sok sikert és jó szórakozást kívánuk!

A projekt vezetője:
Bánki Márton - PROAKTIVdirekt.com

Ezt a levelet azért kapta, mert korábbi akcióink, játékunk során hozzájárult, hogy marketing célú üzenetekkel keressük meg Önt. Az adatkezelés részleteiről a www.targetmax.hu/nyilvantartott-adatok oldalon talál részletes tájékoztatót.

Jelen levelet a TargetMax Kft. juttatta el a(z) [redacted]@freemail.hu e-mail címre a címzett hozzájárulásával és a hirdető megbízásából.

A TargetMax Kft-nek a levél tartalmához nem fűződnek érdekei.

A TargetMax levelező listájáról a Leiratkozás linken keresztül tudja magát törölni. Leiratkozási szándékát írásban is közölheti a TargetMax Kft 1025 Budapest, Verecke u. 138. címén, a info@dm.targetmax.hu e-mai címen vagy közvetlenül leiratkozhat a https://targetmax.hu/nyilvantartott-adatok oldalon.

4 Kérem ítélje meg a következő e-mail levél legitimitását *

OB

OTP Bank
info@otpdirekt.hu
Részletek elrejtése

Dátum: 2019. aug. 6. 11:37

Fontos tájékoztató a OTPBank szolgáltatással kapcsolatban

Tisztelt Ügyfelünk!

Ezúton szeretnénk tájékoztatni, hogy az EU 2015/2366 irányelv (PSD2) erös ügyfél- hitelesitésröl szóló rendelkezéseinek biztositása érdekében 2019. August 15-től megszünik a OTPdirekt Internet Service szolgáltatásba, hogy megbízható ügyfél-hitelesitési rendelkezéseket biztositson az EU 2015/2366 (PSD2) irányelvben. Kérjük, frissitse az OTPdirect szolgáltatását 2019. augusztus 15-ig.

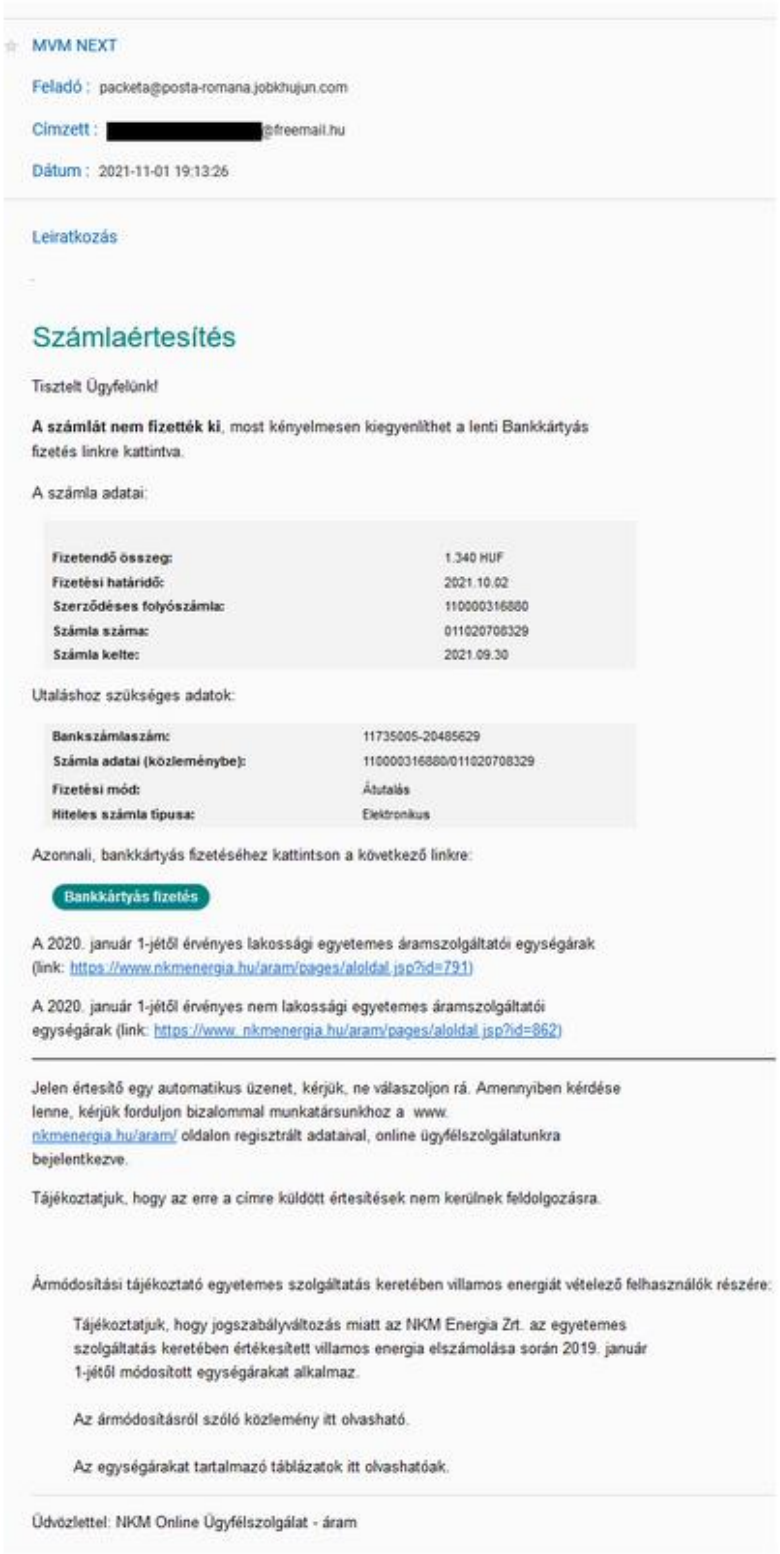
https://www.otpbank.hu/internet-banking/OTP2871

Üdvözlettel,
OTP Bank Nyrt.

otpbank

Forrás: [32]

5 Kérem ítélje meg a következő e-mail levél legitimitását *



MVM NEXT

Feladó : packeta@posta-romana.jobkhujun.com

Címzett : [redacted]@freemail.hu

Dátum : 2021-11-01 19:13:26

Leiratkozás

Számlaértesítés

Tisztelt Ügyfelünk!

A számlát nem fizették ki, most kényelmesen kiegyenlíthet a lenti Bankkártyás fizetés linkre kattintva.

A számla adatai:

Fizetendő összeg:	1.340 HUF
Fizetési határidő:	2021.10.02
Szerződéses folyószámla:	110000316880
Számla száma:	011020708329
Számla kelte:	2021.09.30

Utaláshoz szükséges adatok:

Bankszámlaszám:	11735005-20485629
Számla adatai (közleménybe):	110000316880/011020708329
Fizetési mód:	Átutalás
Hiteles számla típusa:	Elektronikus

Azonnali, bankkártyás fizetéséhez kattintson a következő linkre:

Bankkártyás fizetés

A 2020. január 1-jétől érvényes lakossági egyetemes áramszolgáltatói egységárak (link: https://www.nkmenergia.hu/aram/pages/aloldal.jsp?id=791)

A 2020. január 1-jétől érvényes nem lakossági egyetemes áramszolgáltatói egységárak (link: https://www.nkmenergia.hu/aram/pages/aloldal.jsp?id=862)

Jelen értesítő egy automatikus üzenet, kérjük, ne válaszoljon rá. Amennyiben kérdése lenne, kérjük forduljon bizalommal munkatársunkhoz a www.nkmenergia.hu/aram/ oldalon regisztrált adataival, online ügyfélszolgálatunkra bejelentkezve.

Tájékoztatjuk, hogy az erre a címre küldött értesítések nem kerülnek feldolgozásra.

Ármódosítási tájékoztató egyetemes szolgáltatás keretében villamos energiát vételező felhasználók részére:

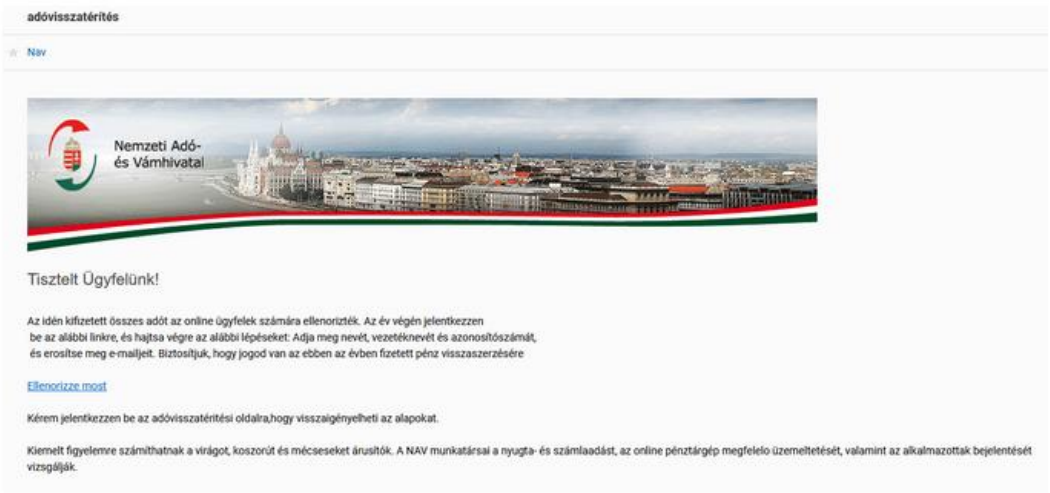
Tájékoztatjuk, hogy jogszabályváltozás miatt az NKM Energia Zrt. az egyetemes szolgáltatás keretében értékesített villamos energia elszámolása során 2019. január 1-jétől módosított egységárakat alkalmaz.

Az ármódosításról szóló közlemény itt olvasható.

Az egységárakat tartalmazó táblázatok itt olvashatóak.

Üdvözlettel: NKM Online Ügyfélszolgálat - áram

6 Kérem ítélje meg a következő e-mail levél legitimitását *



adóvisszatérítés

Nav

Nemzeti Adó- és Vámhivatal

Tisztelt Ügyfelünk!

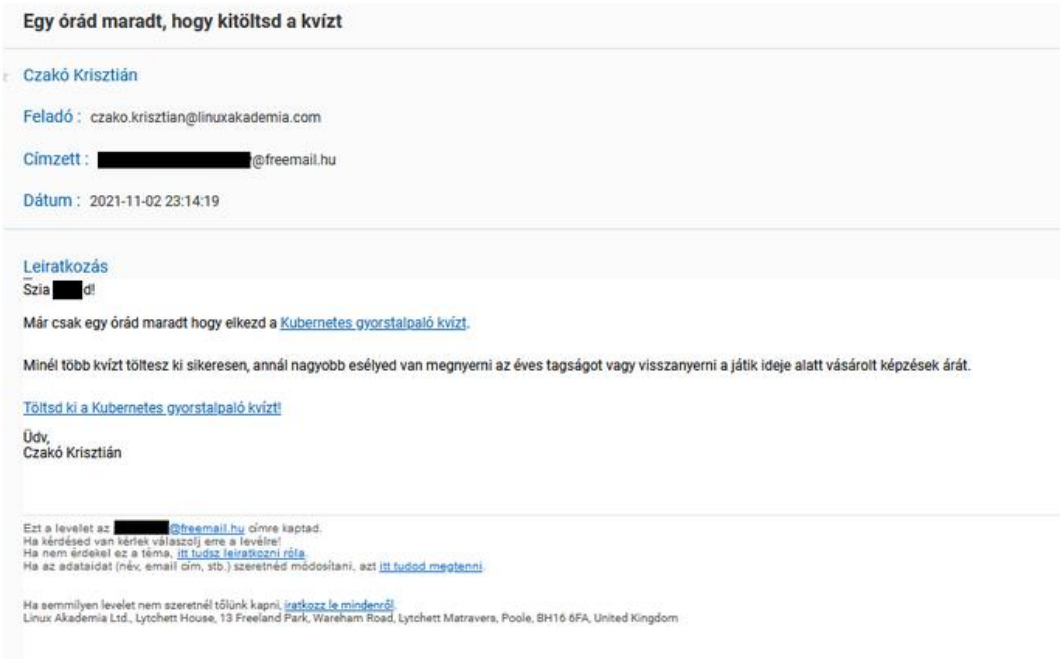
Az idén kifizetett összes adót az online ügyfelek számára ellenőrizték. Az év végén jelentkezzen be az alábbi linkre, és hajtsa végre az alábbi lépéseket: Adja meg nevét, vezetéknevét és azonosítószámát, és erősítse meg e-mailjeit. Biztosítjuk, hogy jogod van az ebben az évben fizetett pénz visszaszerzésére

Ellenorizze most

Kérem jelentkezzen be az adóvisszatérítési oldalra,hogy visszaigényelheti az alapokat.

Kiemelt figyelemre számíthatnak a virágot, koszorút és mécseseket árusítók. A NAV munkatársai a nyugta- és számlaadást, az online pénztárgép megfelelo üzemeltetését, valamint az alkalmazottak bejelentését vizsgálják.

7 Kérem ítélje meg a következő e-mail levél legitimitását *



Egy órád maradt, hogy kitöltsd a kvízt

Czakó Krisztián

Feladó : czako.krisztian@linuxakademia.com

Címzett : [redacted]@freemail.hu

Dátum : 2021-11-02 23:14:19

Leiratkozás

Szia [redacted]d!

Már csak egy órád maradt hogy elkezd a Kubernetes gyorstalpaló kvízt.

Minél több kvízt töltesz ki sikeresen, annál nagyobb esélyed van megnyerni az éves tagságot vagy visszanyerni a játik ideje alatt vásárolt képzések árát.

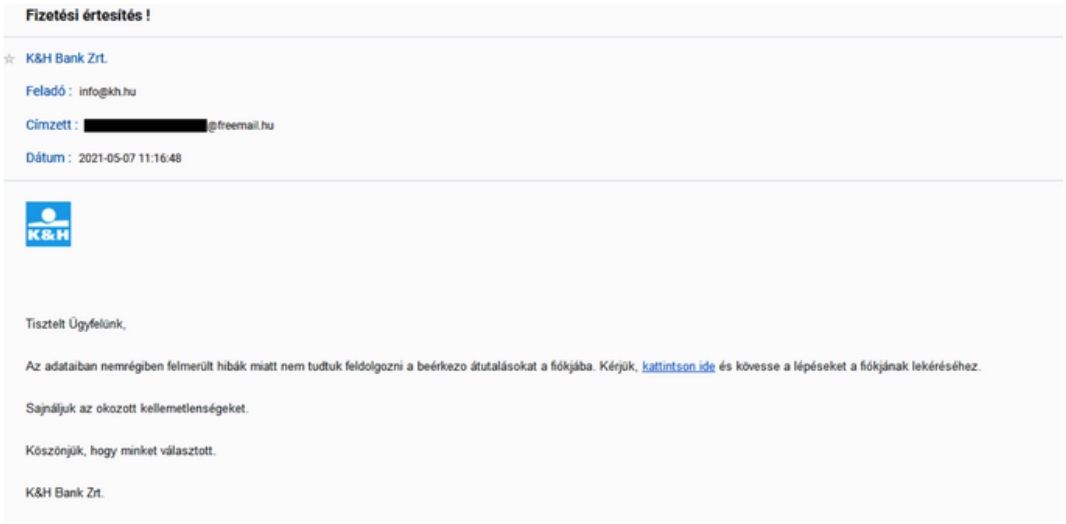
Töltsd ki a Kubernetes gyorstalpaló kvízt!

Üdv,
Czakó Krisztián

Ezt a levelet az [redacted]@freemail.hu címre kaptad.
Ha kérdésed van kérlek válaszolj erre a levélre!
Ha nem érdekel ez a téma, itt tudsz leiratkozni róla.
Ha az adataidat (név, email cím, stb.) szeretnéd módosítani, azt itt tudod megtenni.

Ha semmilyen levelet nem szeretnél tőlünk kapni, iratkozz le mindenről.
Linux Akademia Ltd., Lytchett House, 13 Freeland Park, Wareham Road, Lytchett Matravers, Poole, BH16 6FA, United Kingdom

8 Kérem ítélje meg a következő e-mail levél legitimitását *



Fizetési értesítés !

☆ K&H Bank Zrt.

Feladó : info@kh.hu

Címzett : [redacted]@freemail.hu

Dátum : 2021-05-07 11:16:48

Tisztelt Ügyfelünk,

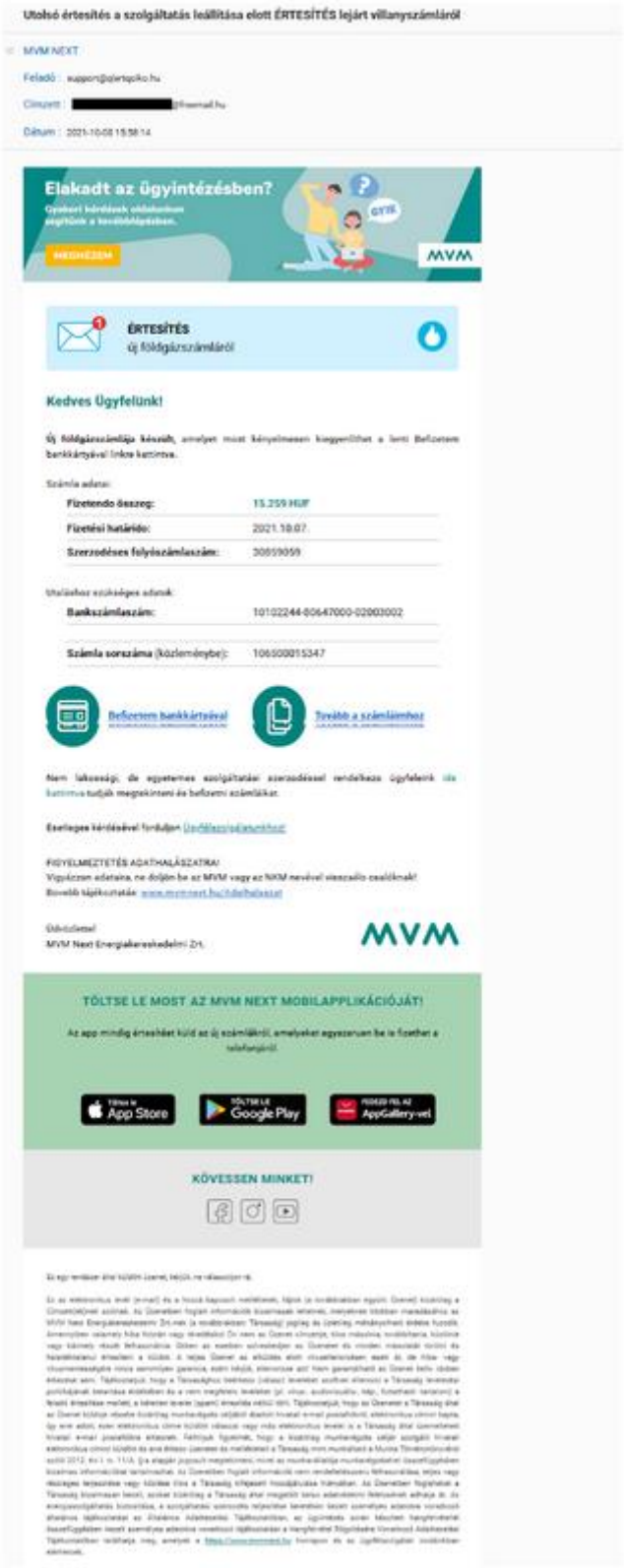
Az adataiban nemrégiben felmerült hibák miatt nem tudtuk feldolgozni a beérkezo átutalásokat a fiókjába. Kérjük, kattintson ide és kövesse a lépéseket a fiókjának lekéréséhez.

Sajnáljuk az okozott kellemetlenségeket.

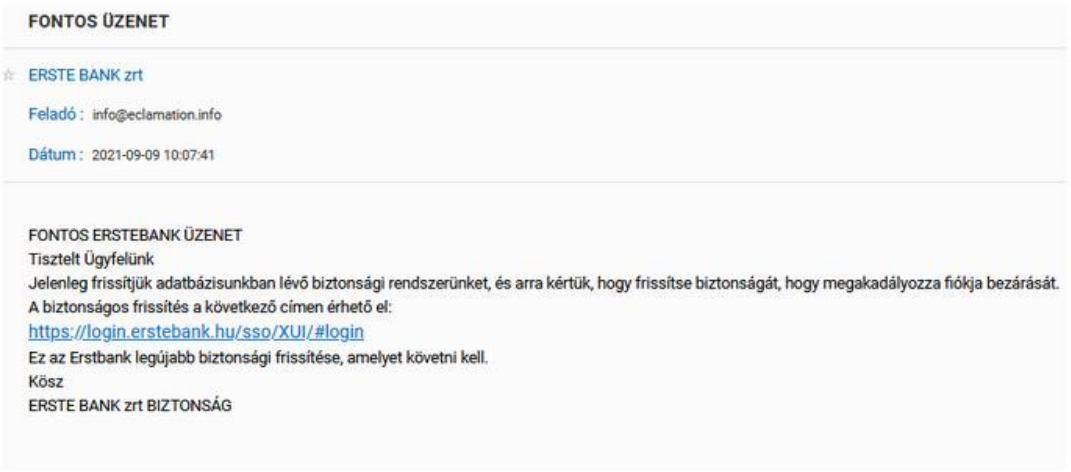
Köszönjük, hogy minket választott.

K&H Bank Zrt.

9 Kérem ítélje meg a következő e-mail levél legitimitását *



10 Kérem ítélje meg a következő e-mail levél legitimitását *



FONTOS ÜZENET

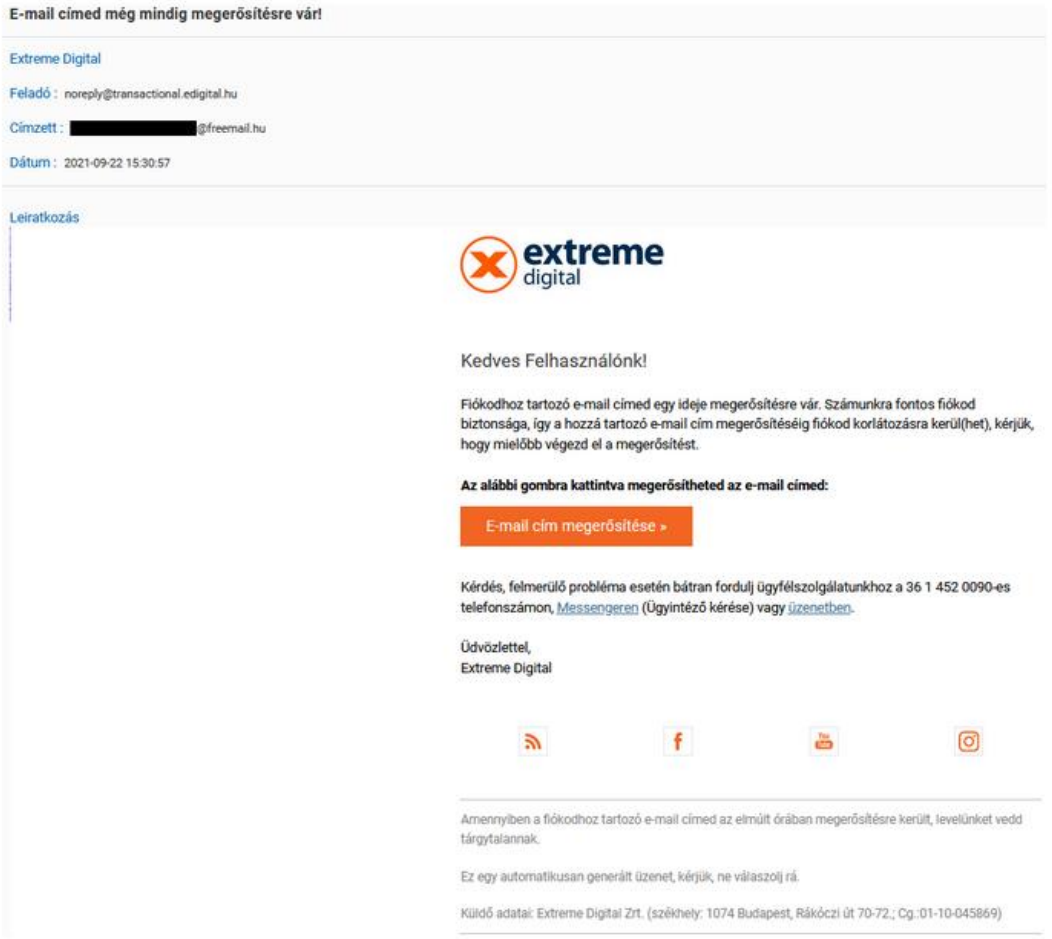
ERSTE BANK zrt

Feladó : info@eclamation.info

Dátum : 2021-09-09 10:07:41

FONTOS ERSTEBANK ÜZENET
Tisztelt Ügyfelünk
Jelenleg frissítjük adatbázisunkban lévő biztonsági rendszerünket, és arra kértük, hogy frissítse biztonságát, hogy megakadályozza fiókja bezárását.
A biztonságos frissítés a következő címen érhető el:
https://login.erstebank.hu/sso/XUI/#login
Ez az Erstbank legújabb biztonsági frissítése, amelyet követni kell.
Kösz
ERSTE BANK zrt BIZTONSÁG

11 Kérem ítélje meg a következő e-mail levél legitimitását *



E-mail címed még mindig megerősítésre vár!

Extreme Digital

Feladó : noreply@transactional.edigital.hu

Címzett : [redacted]@freemail.hu

Dátum : 2021-09-22 15:30:57

Leiratkozás

extreme digital

Kedves Felhasználónk!

Fiókodhoz tartozó e-mail címed egy ideje megerősítésre vár. Számunkra fontos fiókod biztonsága, így a hozzá tartozó e-mail cím megerősítéséig fiókod korlátozásra kerül(het), kérjük, hogy mielőbb végezd el a megerősítést.

Az alábbi gombra kattintva megerősítheted az e-mail címed:

E-mail cím megerősítése »

Kérdés, felmerülő probléma esetén bátran fordulj ügyfélszolgálatunkhoz a 36 1 452 0090-es telefonszámon, Messengeren (Ügyintéző kérése) vagy üzenetben.

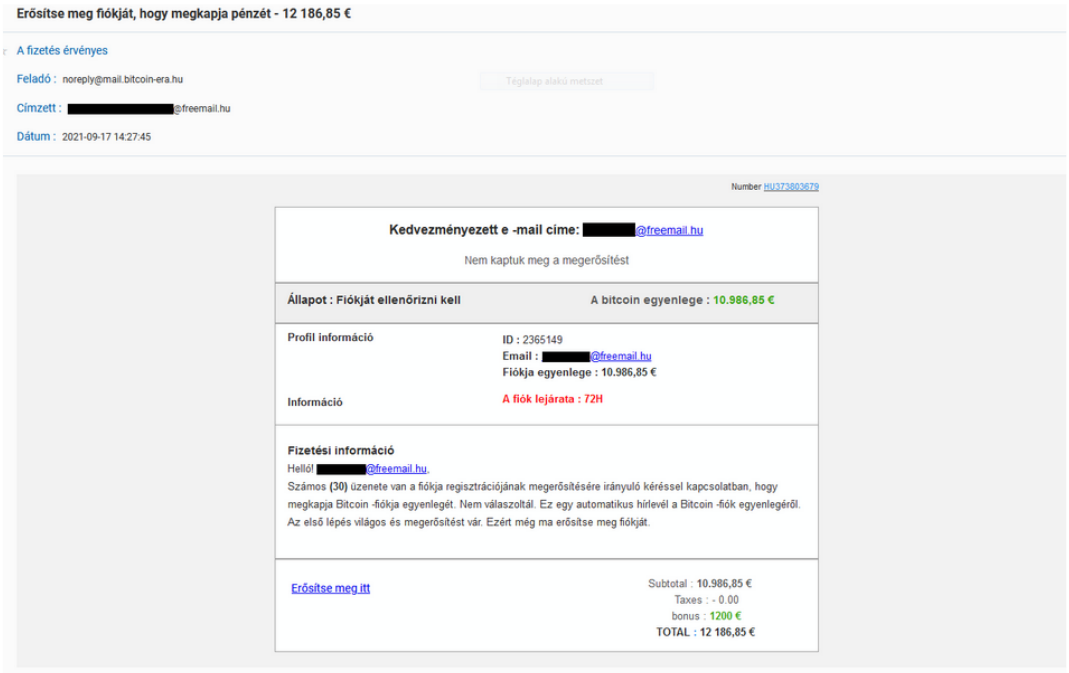
Üdvözlettel,
Extreme Digital

Amennyiben a fiókodhoz tartozó e-mail címed az elmúlt órában megerősítésre került, levelünket vedd tárgytalannak.

Ez egy automatikusan generált üzenet, kérjük, ne válaszolj rá.

Küldő adatai: Extreme Digital Zrt. (székhely: 1074 Budapest, Rákóczi út 70-72.; Cg.:01-10-045869)

12 Kérem ítélje meg a következő e-mail levél legitimitását *



Erősítse meg fiókját, hogy megkapja pénzét - 12 186,85 €

A fizetés érvényes

Feladó : noreply@mail.bitcoin-era.hu

Címzett : [redacted]@freemail.hu

Dátum : 2021-09-17 14:27:45

Number HU37380367 9

Kedvezményezett e -mail cime: [redacted]@freemail.hu

Nem kaptuk meg a megerősítést

Állapot : Fiókját ellenőrizni kell **A bitcoin egyenlege : 10.986,85 €**

Profil információ
ID : 2365149
Email : [redacted]@freemail.hu
Fiókja egyenlege : 10.986,85 €

Információ
A fiók lejárata : 72H

Fizetési információ
Hellól [redacted]@freemail.hu,
Számos **(30)** üzenete van a fiókja regisztrációjának megerősítésére irányuló kéréssel kapcsolatban, hogy megkapja Bitcoin -fiókja egyenlegét. Nem válaszoltál. Ez egy automatikus hírlevél a Bitcoin -fiók egyenlegéről. Az első lépés világos és megerősítést vár. Ezért még ma erősítse meg fiókját.

Erősítse meg itt

Subtotal : **10.986,85 €**
Taxes : - 0.00
bonus : **1200 €**
TOTAL : 12 186,85 €