

Pécsi Tudományegyetem  
Műszaki és Informatikai kar  
Rendszer és Szoftvertechnológiai Tanszék

A MESTERSÉGES INTELLIGENCIA ÉS SOCIAL ENGINEERING,  
AVAGY A PEOPLE PREDICTION KUTATÁSA  
Tolnai Máté Gergely

Készítette: Tolnai Máté Gergely  
Évfolyam: Mérnökinformatikus BSC 4.

Belső konzulens: Gyurák Gábor  
Beosztása: Mesteroktató

Pécs  
2023

# TARTALOMJEGYZÉK

## 1. Tartalom

|        |                                            |    |
|--------|--------------------------------------------|----|
| 2.     | Bevezetés és célkitűzések:.....            | 3  |
| 2.1.   | Elméleti és gyakorlati jelentősége:.....   | 3  |
| 2.2.   | Célkitűzések: .....                        | 3  |
| 2.3.   | Vizsgálati módszerek: .....                | 4  |
| 3.     | A módszerek egy ismertetése példákkal..... | 6  |
| 3.1.   | AI elhelyezkedése .....                    | 6  |
| 3.2.   | Scanning.....                              | 6  |
| 3.2.1. | Phishing/Spear Phishing .....              | 6  |
| 3.3.   | Reconnaissance.....                        | 8  |
| 3.4.   | Exploitation .....                         | 8  |
| 3.4.1. | Impersonation .....                        | 8  |
| 3.4.1. | A program háttere .....                    | 10 |
| 3.4.2. | Megkötések.....                            | 10 |
| 3.4.3. | A program működése.....                    | 12 |
| 3.4.4. | Pretexting.....                            | 14 |
| 3.5.   | Maintaining Access.....                    | 17 |
| 3.5.1. | A program alkalmazása .....                | 17 |
| 3.6.   | Covering Tracks.....                       | 19 |
| 4.     | A kutatás eredménye.....                   | 20 |
| 5.     | Összefoglalás .....                        | 22 |
| 6.     | Köszönetnyilvánítás.....                   | 23 |
| 7.     | Nyilatkozat.....                           | 25 |

## 2. Bevezetés és célkitűzések:

### 2.1. Elméleti és gyakorlati jelentősége:

Minden védelmi rendszer leggyengébb pontja az ember, mint szokták mondani. A social engineering pszichológiai manipuláció alkalmazása, amellyel ráveszik az embereket arra, hogy olyan információkat adjanak ki, tetteket hajtsanak végre, amelyeket általában nem szoktak.[1]

A „2020-as Verizon Data Breach Investigations Report” [2] szerint az adathalászat (phishing) az első fenyegetési művelet a jogsértésekben, és a számítógépes bűnözők által használt második támadási vektor. A 2022-es riport szerint a támadások 82% emberi elemet érintő jogsértés által következett be, beleértve az SE támadásokat, hibákat és visszaéléseket.

A mesterséges intelligencia konzumer változatainak megjelenésével egy olyan támadási vektor jelent meg, amivel eddig nem számolt a kiberbiztonság védelmi oldala. Az egyszerű social engineering támadások indításához szükséges eszközök és módszerek túl könnyen hozzáférhetővé váltak a mai modern technológiai adottságoknak köszönhetően. A személyes adatok, mint például a név, születési dátum, e-mail cím és telefonszám, könnyen elérhetőek az interneten, amelyeket a támadók felhasználhatnak az áldozatok megtévesztése érdekében. Az interneten számos forrás található a támadók számára, ahol megtanulhatják ezeknek az információknak kihasználására alkalmas támadásoknak az alapjait és a sikeres végrehajtásukhoz szükséges technikákat. Kutatásom során kontrollált környezetben egy AI irányított prediktív analízis program fejlesztésével és egy több mint fél éven át tartó social engineering kutatással prezentálom ennek hatékonyságát. A vizsgálatok eredményei segíthetnek a kiberbiztonsági szakembereknek és döntéshozóknak a megfelelő védelmi stratégiák kidolgozásában és a digitális tér fenntartható fejlődésének támogatásában.

### 2.2. Célkitűzések:

Az AI és Social Engineering kölcsönhatásának elemzése: Vizsgálni fogom, hogyan befolyásolják az AI rendszerek a társadalmi manipuláció hatékonyságát, és milyen módon használják ki a személyes adatokat a People Prediction kutatások során.

Etikai kérdések kibontakoztatása: A kutatás során felmerülő etikai problémákat és kihívásokat részletezem, különös tekintettel az egyének magánéletére és jogaira.

### 2.3. Vizsgálati módszerek:

A kutatásom szisztematikus irodalomáttekintést, esettanulmányokat és kísérleteket foglal magába. Az AI és Social Engineering összetett témák, ezért a kvantitatív és kvalitatív módszerek kombinációja segít megfelelően felfedni a kutatás célkitűzéseit. A szisztematikus irodalomáttekintés segít az elméleti keretek kialakításában, míg az esettanulmányok és kísérletek konkrét példákon keresztül teszik lehetővé az eredmények gyakorlati alkalmazását. Fontos megjegyezni, hogy a pszichológiai oldalát a social engineering támadásoknak már tanulmányoztam egyetemi, és autodidakta módon is, ezeket a megszerzett tudásokat fogom összehasonlítani az AI nyújtotta lehetőségekkel, validálni azok pontosságát.

### 3. Irodalmi áttekintés:

A social engineering támadások komoly kockázatot jelentenek a szervezetek biztonságára. Több nagy profilú kiber-támadás, például a RSA, JP Morgan, AT&T, az ukrán energiahálózat stb., kihasználta a social engineering technikákat az adott szervezetek rendszereibe való belépési pontként. A támadók számos taktikát alkalmaznak, az egyszerű személyazonosság-utánpótlástól kezdve a bonyolult, Hollywood-i cselekményhez méltó, többrétegű megtévesztésekig, amelyek célja egy célpont kényszerítése kényes információk kiadására vagy egy rosszindulatú terheléssel való interakcióra.

## 4. A módszerek egy ismertetése példákkal

A módszerek egy része nagyban azonosítható az cyber killchain 5 fáziséval. Ezeken a lépéseken fogom végig vezetni az kutatásom, és megmutatni, hogy miképp segített az AI ezeket a lépéseket végrehajtani.

Ezek a fázisok:

1. Reconnaissance, adatgyűjtés
2. Scanning, sebezhetőség elemzés
3. Gaining Access, exploitálás
4. Maintaining Access, rendszerfenntartás
5. Covering Tracks, nyomok eltakarása

Első lépésként a reconnaissance és scanning fázist vizsgáltam. Kerestem egy megnevezett - akár fiktív - felsőoktatási intézményt amiről összegyűjtöttem minden publikusan fellelhető adatot. Az adatgyűjtés és scanning fázis sikeres volt.

**Minden egyezés a valósággal csak a véletlen műve.**

### 4.1. AI elhelyezkedése

Kutatásom során az összes lépés végrehajtásához szükséges információkat a mesterséges intelligencia egy ingyenes változata formálta meg, alakította ki. Ezeket a megadott lépéseket hasonlítottam össze már meglévő és alkalmazott social engineering támadásokkal, így prezentálni tudtam ezeknek a módszereknek a pontosságát és hatékonyságát.

### 4.2. Scanning

#### 4.2.1. Phishing/Spear Phishing

Az phishing (adathalászat) általában tömeges e-maileket vagy üzeneteket foglal magában, amelyeket nagymennyiségű embereknek küldenek ki azzal a céllal, hogy a lehető legtöbb címzettet rávegyék, hogy rákattintsanak egy rosszindulatú linkre, letöltsenek egy mellékletet, vagy érzékeny információkat, például jelszavakat vagy hitelkártyaadatokat fedjenek fel. Az e-maileket gyakran úgy alakítják ki, hogy megbízható forrásból, például bankból, közösségi média platformból vagy e-kereskedelmi webhelyről érkezzenek, és sürgősségi vagy félelmet keltő taktikákat alkalmazhatnak, hogy gyors cselekvésre ösztönözzék a címzettet.

A spear phishing (lándzsás adathalászat) viszont az adathalász támadások célzottabb formája. Ahelyett, hogy tömeges e-maileket küldene emberek nagy csoportjának, a támadó egy adott személyre vagy személyek csoportjára összpontosít. A támadó kiterjedt kutatást végezhet a célpont(ok)on, hogy személyes adatokat gyűjtsön, például nevüket, beosztásukat vagy legutóbbi tevékenységeiket, és ezeket az információkat egy rendkívül személyre szabott és meggyőző üzenet létrehozására használja fel. Az adathalászat célja gyakran az érzékeny adatokhoz vagy rendszerekhez való hozzáférés.

### 4.3. Reconnaissance

A reconnaissance fázisból kinyert adatok által a spear phishing támadás volt a legerfektiívebb.

*"Az embernek két mozgatórugója van: az egyik a szükségletek kielégítése, a másik a szükségletek növelése. Az első cél, hogy megszabaduljunk a fájdalomtól, vagyis az éhségtől, a szomjtól, az unalomtól, a félelemtől. Azonban ha ezek a szükségletek kielégültek, akkor valami nagyobbat akarunk elérni, mint csak azoknak az elkerülését. Ez az önmegvalósítás vágya. És a legmagasabb szintű önmegvalósítás az, amikor az ember képes másokon segíteni."* [3] (4.3.1)

A [REDACTED] egyetemen vannak segítő hallgató szervezetek?

A [REDACTED] számos hallgatói szervezetet és szolgáltatást kínál, amelyek segítséget nyújtanak a diákoknak. Ezek a szervezetek és szolgáltatások több területen működhetnek, például oktatás, karrierfejlesztés, diákélet, egészségügy, és sok más területen.

#### 4.3.1 Segítők

Ebből az elvből kiindulva, mikor megláttam, hogy az intézmény weboldalán található „Mentor szervezet” és egy Hallgatói Önkormányzat, összevettem a két szervezetben található neveket és több egyezést is találtam. Érdekes megjegyezni, hogy a mentor szervezet oldalán 12 tagból 9 tagnak a személyes emailcíme van megadva az oldalon. Megvoltak az áldozatok.

### 4.4. Exploitation

#### 4.4.1. Impersonation

Az impersonation (megszemélyesítés) típusú támadások során az elkövető álcázza magát, hogy közel kerüljön az áldozathoz, majd ezt a bizalmat felhasználva manipulálja őt. Ez magában foglalhatja azt, hogy kiadja magát banki képviselőnek, ügyfélszolgálati ügynöknek vagy egy kollégának. Az áldozat azt hiheti, hogy az illető az, akinek mondja magát, és így nagyobb valószínűséggel teszi azt, amit az elkövető akar. Ez az áldozat hitén alapul.

Magyarországon a legnépszerűbb közösségi média oldalak a Facebook és a YouTube [4]. Megszemélyesítéssel támadás során figyelembe vettem a 1986-ban megjelent "Women receive more help than men from same-sex and cross-sex dyads" című tanulmányt [5],

ami arra a következtetésre jutott, hogy a nők nagyobb valószínűséggel kapnak segítséget másoktól, mert a segítségkérésük társadalmilag elfogadottabb, mint a férfiaké. Ezen okokból adódóan készítettem el egy női personát facebookon, aki demográfiaailag tökéletesen beleillik az (oktatási)intézmény képébe, és az áldozatok scope-jába. A neve az 50 leggyakoribb keresztné és vezetéknévekből állt össze, a születési helye, lakhelye és gimnáziumának helye egy távoli nagyváros.

Levelezős hallgató, másodéves, dolgozik egyetem mellett, nem volt sok ideje ismerősöket szerezni ebből adódóan. Személyének utóbbi pontja fontos volt a szimpátia és elesettségérzés növelésében. Fontos, hogy informatikus hallgató, mivel egy 2015-ben a Journal of Vocational Behavior-ben [4] megjelent tanulmány szerint az IT iparágban nagyobb az introvertáltak aránya, mint az általános népességben. Profilképének (4.4.1.1). egy, ingyenes AI program (Canva) generátorát alkalmaztam, amivel elértem, hogy ne találja meg a fordított képkeresés. Borítóképe egy intézmény helyének megfelelő helyről készített saját fotó, aminek a metaadatait módosítottam.



**4.4.1.1 Somogyi Enikő**

#### 4.4.2. A program háttere

A már említett AI generált üzenetek mögött a kutatásom egyik alappillére, egy beszélgetés kezdeményezést és predikciót támogató script írása volt. Az emberek kiszámíthatóak, nagyobb valószínűséggel válaszolnak, minél több adatot tudunk róluk, tudunk velük pontosan közölni. A fejlett nyelvi rendszerek képesek tanulni a célszemély kommunikációs stílusáról, írásbeli kifejezéseiről. Az algoritmusok elemzik a cél egyének digitális lábnyomát, érdeklődési körét, kapcsolatait és online viselkedését. Ennek eredményeként a pretexting üzenetek személyre szabottak lehetnek, növelve a siker esélyét. Ez lehetővé teszi, hogy a pretextek természetesebben és hihetőbben illeszkedjenek a célszemély kommunikációjához, növelve ezzel az átverés sikerességét.

A program egy python script ami a BeautifulSoup4 könyvtárat használja alapul ami HTML és XML dokumentumok elemzésére. Ez egy elemzőfát hoz létre a beolvasott oldalakhoz, amelyet fel lehet használni adatok kinyerésére HTML-ből, ami hasznos a web scrapeléshez.

#### 4.4.3. Megkötések

Bár a könyvtár hasznos, a Facebook adatpolitikai érdekeit és irányelveit tekintve több faktort is figyelembe kellett venni:

##### Automatizált adatgyűjtés:

Facebook tiltja a webscrapinget vagy más automatizált eszközök használatát az adatok gyűjtésére a platformról anélkül, hogy erre kifejezett engedélyt kapnál. Ez vonatkozik az egyéni felhasználók, csoportok és oldalak adataira egyaránt.

##### Felhasználói adatok védelme:

Az adatpolitika hangsúlyozza a felhasználói adatok védelmét és azt, hogy azokat csak azok a módon lehet gyűjteni és felhasználni, amelyek a Facebook irányelveivel összhangban állnak. Az engedély nélküli webscraping kockázatot jelenthet a felhasználók személyes adatainak jogosulatlan elérésére.

Hogy megfeleljek a jogi elvárások ezen részének, csak olyan profilokon futtattam a scriptet, akiknek a nyilvános adatait ugyan úgy elértem, miután visszajelöltek volna, tehát privát információval való visszaélés nem történt Open Source Intelligence (OSINT)-nak minősült, jogszabályt nem sértve. Az automatizálást tekintve, webhelyről történő

adatscraping nem ment végbe, mivel a profilokat manuálisan töltöttem le, miután elfogadták a baráti felkérést.

#### 4.4.4. A program működése

Egy profil letöltése manuálisan, elnavigálva a felhasználó oldalára majd jobbklikkel „mentés másként” -al történik. Ez letölti a profil alapvető tartalmát, amit látna az ember ha rákattintana mint ismerőse (például: <http://facebook.com/profile.php?=73322363> ). Lényegében egy nyers HTML-filet. A program egy TKinter felugróablakból felajánlja, hogy válasszuk ki az elemezni kívánt profilt (4.4.4.1).

```
root = tk.Tk()
root.withdraw()

html_file_path = filedialog.askopenfilename(title="Select an HTML file", filetypes=[("HTML Files", "*.html")])

if not html_file_path:
    print("No file selected. Exiting.")
    exit()

with open(html_file_path, 'r', encoding='utf-8') as file:
    html_content = file.read()
```

##### 4.4.4.1 Profilválasztás

Innen átadja a kinyert információt egy másik functionnak, ami elvégzi az adatok kinyerését. A facebook, a gyorsabb futás (és a webscraping megnehezítésének érdekében) már nem használ olyan classokat mint „post” vagy „content” hanem ember számára olvashatatlan classok sokaságával látja el az adott elemet. Ez megnehezítette a nyers adatok kiszűrését, de szerencsére megfelelő regexel vagy jól felkonfigurált BeautifulSoup functionnal, kilehet nyerni az adatok nagyrészét (4.4.4.2):

```
def get_text_from_span_and_a(html_content):
    soup = BeautifulSoup(html_content, 'html.parser')
    span_and_a_tags = soup.find_all(['span', 'a'])

    text_content = ""
    for tag in span_and_a_tags:
        if not tag.get('class'):
            text = tag.get_text(separator='\n', strip=True)
            if len(text) > 2:
                text_content += text + '\n'
        elif 'tags' in tag.get('class'):
            text = tag.get_text(separator='\n', strip=True)
            if len(text) > 2:
                text_content += text + '\n'

    return text_content
```

##### 4.4.4.2 Adatnyerés

Egy tesztprofilon való lefuttatás alapján az alábbi adatokat sikerült kinyerni egy profilból (4.4.4.3):

```
Filtered Text Content:
38 közös ismerős
[REDACTED]
Kezdés: 2022.
Muraszemenye
Nagykanizsa
Mikulásház a Laczkó Ranchon Tárnokon
[REDACTED]
Black Veil Brides, Halestorm | Budapest 2023
DAAD Gathering 2024
Ed Sheeran - Puskás Aréna, Budapest 2024
OZORA Festival 2024
```

#### 4.4.4.3 Nyert adatok

Látszik a tesztprofil tanulmányára, mikor kezdte, hol lakik, milyen programokon szeretne részt venni, milyen beszélgetési (akár közös) témákat oszt meg magáról. Ezeket az adatokat továbbítva egy ingyenes AI nyelvi modellnek, megfelelő promptlással, az alábbi válaszokat kapjuk (a teljesség igénye nélkül) (4.4.4.4):

```
1. Közös Ismerősök:
• Mivel 38 közös ismerősötök van, érdemes lehet említést tenni ezekről az ismerősökről.
  Például: "Szia! Láttam, hogy rengeteg közös ismerősünk van, például XY és Z. Hogyan ismeritek egymást?"

2. [REDACTED]
• Mivel mindketten a [REDACTED] kezdtétek el a tanulmányaitokat 2022-
  ben, ezen az alapon említheted, hogy milyen élményeket szereztek ott. "Helló! Láttam,
  hogy mindketten a [REDACTED] kezdtük a tanulmányainkat 2022-ben.
  Milyen szakon tanulsz?"

3. Események és Koncertek:
• Látszik, hogy részt vettek közös eseményeken, mint a Gólyabál vagy a koncertek
  ([REDACTED], stb.). Említheted, hogy te is ott voltál, és megoszthatod a
  tapasztalataidat vagy kérdezheted, hogy neki milyen élményei voltak ezeken az
  eseményeken.

4. Helyek:
• Muraszemenye, Nagykanizsa, és a Mikulásház a Laczkó Ranchon Tárnokon is közös
  pontok, amelyekről beszélgethetsz. Például: "Láttam, hogy kapcsolódsz
  Muraszemenyéhez és Nagykanizsához. Szeretem ezeket a helyeket, van valami kedvenc
  emléked?"
```

#### 4.4.4.4 Beszélgetés indítás

#### 4.4.5. Pretexting

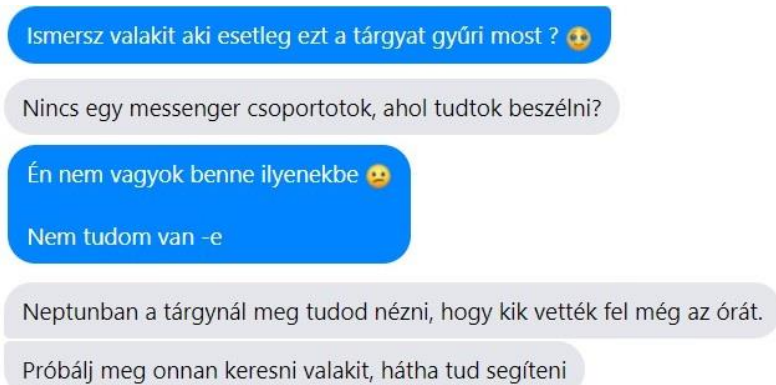
A pretext támadás („ürügyes” támadás) során a támadó először információkat gyűjt a célponttól, majd olyan jogosnak tűnő helyzetet hoz létre, amely alátámasztja annak szükségességét, hogy a célpont bizalmas információkat osszon meg, vagy olyan lépéseket tegyen, amelyek segíthetik a támadót. Az ürügként szolgáló támadások gyakran nagyon célzottak és személyre szabottak, az áldozatok megtévesztésére és érzelmeik kihasználására támaszkodnak. Az ilyen támadások általában sikeresek lehetnek, mert a támadók által létrehozott történetek valódinak és meggyőzőnek tűnnek a célpont számára.

A példákban jelölt üzeneteket AI írta, minimális átdolgozással (esetekben anélkül) is kérdés nélkül elfogadták az üzeneteket. Ezen előre betáplált adatok alapján küldtem a további üzeneteket (4.4.5.1):

1. **Nature of the Situation:** A 21-year-old IT engineer student is likely to offer help when they encounter situations where assistance is required, regardless of the person's characteristics. For example, if someone is in distress or facing technical difficulties, the student may be more inclined to provide assistance.
2. **Shared Interests:** A common interest, such as an interest in IT, can create a basis for connection and willingness to help. If the woman is a fellow student or shares an interest in technology, the student may be more likely to offer assistance.
3. **Communication:** Effective communication plays a significant role. If the woman communicates her needs or requests for help, the student is more likely to provide assistance.
4. **Friendship or Acquaintance:** Existing friendships or acquaintanceships can influence the willingness to help. Students may be more inclined to assist friends or acquaintances they know.
5. **Empathy and Altruism:** A student's willingness to help is often driven by empathy and altruism. If they genuinely care about the well-being of others, they may be more likely to assist women or anyone else in need.
6. **Technical Expertise:** In the context of IT, a 21-year-old IT engineer student may be more inclined to help if they have the technical expertise and knowledge to address the specific issue.

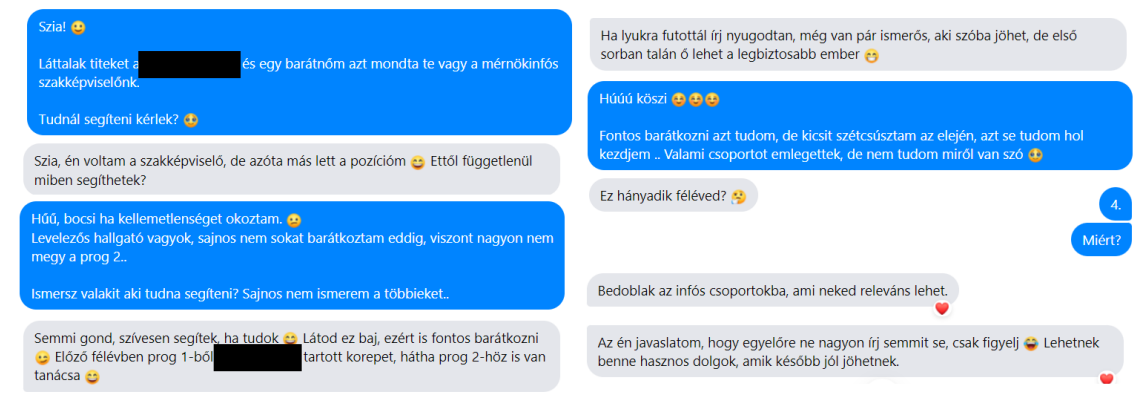
##### 4.4.5.1 Tanácsok

A közös tagok között volt 3 fő akik a personának ideális támadási pontjai voltak. Elsődleges célom az információ gyűjtése volt, megtudni milyen szociális körök vannak, mennyire nyitottak. Egy általánosnak mondható informatikai problémával kerestem fel az első áldozatot (4.4.5.2).



#### 4.4.5.2 információ szerzése

Feltételezve, hogy léteznek ezek a csoportok másodlagos célom a hallgatóság széleskörű elérése volt, „ismerős szerzés”. Ehhez, bekellett jussak hallgatói csoportokba. Ezt az egyik áldozaton keresztül értem el, az alábbi ábra szerint (4.4.5.3):



#### 4.4.5.3. integrálódás

Célomat elértem, kettő hallgatói csoportba is felvettek, így van lehetőségem az összes csoportbéli hallgatót elérni.

A vizsgált intézmény több elérhetőségét is felkeresve emaileket is írtam, hogy több információt tudjak meg. Ezekben az esetekben nem volt szükség a program használatára, az üzenetek nagyrésze módosítatlanul került elküldésre (4.4.5.4):

Tisztelt [REDACTED]!

A nevem [REDACTED] MIK-es mérnökinformatikus hallgató vagyok.

A folyosón fél füllel hallottam, hogy lenne lehetőség laborfelügyeletre mint hallgató.

Amennyiben van lehetőség, szeretnék először is érdeklődni, majd jelentkezni erre a lehetőségre önkénteskedni, vagy akár ha csak segíteni segíthetnék az nagyon sokat jelentene nekem, nagyon szeretnék beletanulni ebbe az egészbe! :)

Gyors tanuló vagyok és nagyon hálás lennék!

Válaszát előre is köszönöm!

Tisztelettel:

[REDACTED]

#### **4.4.5.4 Email példa**

## 4.5. Maintaining Access

### 4.5.1. A program alkalmazása

A rendszerfenntartás fontos volt, hogy a kutatás több hónapos lefolyása során fenntartsa az emberek érdeklődését, elhiggyék, hogy a persona létezik. A hallgatói csoportokban kommunikáltam, a scanning fázisban talált 3 fővel beszélgettem AI generált üzenetekkel.

Az AI tanácsait megfogadva szimpátia elnyeréssel próbáltam közelebb keríteni magamhoz az embereket (4.5.1.1).



#### 4.5.1.1 Szimpátia példa

Közben vizsgáltam a hallgatói aktivitást, vártam a válaszüzeneteket, amik idővel meg is érkeztek (4.5.1.2):

Kedves Enikő!

[REDACTED]nak hívják az illető Urat, hivatkozz rám nyugodtan!  
[REDACTED]@ [REDACTED].hu

Sok sikert!

[REDACTED]

#### 4.5.1.2 Válasz üzenet

## 4.6. Covering Tracks

„A "ghostolás" olyan tevékenységet jelent, amikor valaki egy másik személyt elkerüli vagy minimalizálja a kapcsolatot, hogy ne tűnjön fel neki az online vagy offline életben.„  
Az AI tanácsára az alábbi lépésekkel értem el, hogy fel se tűnjön az embereknek hogy egy hét alatt a persona felszívódik (4.6.1):

### **Üzenetek elkerülése:**

- Ha szeretnéd minimalizálni az üzenetváltásokat valakivel, nem válaszolhatsz az üzeneteire vagy hosszabb időre el is hagyhatod a beszélgetést. Ne feledd, hogy mindig fontos tiszteletteljes maradni.

### **Csoportok vagy rendezvények elkerülése:**

- Ha a másik személy részt vesz olyan csoportokban vagy eseményeken, amelyeken te is, akkor fontolóra veheted ezek elkerülését vagy csoportokból való kilépést.

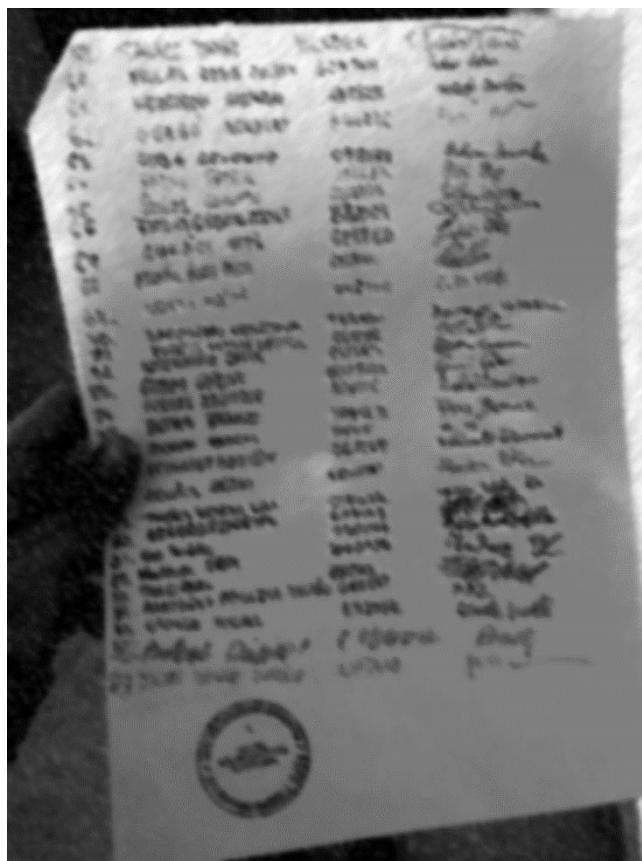
### 4.6.1 Ghosting

## 5. A kutatás eredménye

Az elvégzett kutatás rendkívül sikeresnek bizonyult, amelyre több mint 100 résztvevő pozitív válaszreakcióval reagált. Az elfogadók túlnyomó többsége fiú volt, ami további érdekes szempontokat adott az eredmények elemzéséhez.

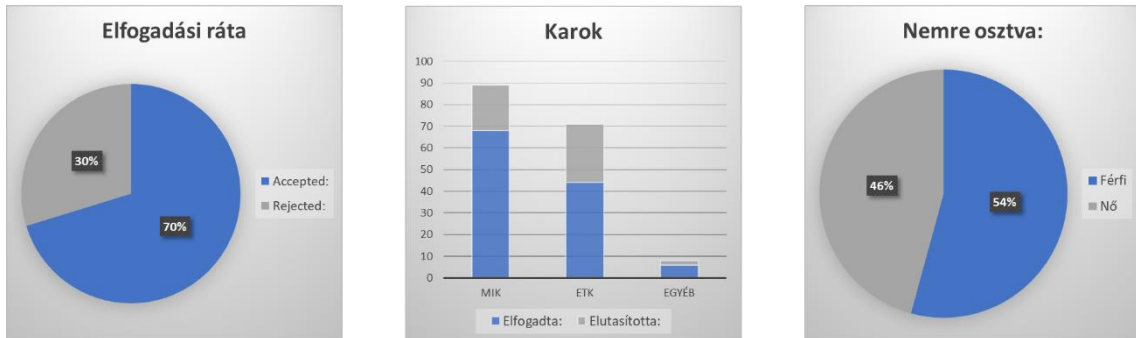
### 5.1. Statisztikák

A kutatás során számos résztvevő hozzáférést biztosított, a bizalmas egyetemi fájlokhoz. Az adatokat törvényesen és etikusán kezeltük, visszaélés velük nem történt, az adatok másolása nem történt meg. A kutatás eredményeit tekintve, a nagyobb adatmennyiség és a résztvevők sokfélesége lehetővé tette számunkra, hogy mélyebb betekintést nyerjünk az egyetemi folyamatokba és az érintett hallgatók mindennapjaiba. A több mint 60 bizalmas file között megtalálható több hallgató személyes adata, elérhetősége, lakcíme, belső felhasználásra készült egyetemi filek, belépési azonosítók vagy akár vicces (és kompromitálásra alkalmas) képek. Az alábbi fiktív képen több mint 25 hallgató aláírása, neptunkódja és neve található meg(5.1.1):



5.1.1 Eredmények

Ezenkívül fontos megjegyezni, hogy a korosztályok eloszlásában a segítségnyújtással kapcsolatban nem mutatkozott különbség. Az eredmények azt mutatják, hogy a segítségnyújtás iránti hajlandóság és a kutatásba való aktív részvétel nem függött össze a résztvevők életkorával, nemével. (5.1.2)



**5.1.2 Statisztikák**

## 5.2. Jogi háttér

A kutatás megkívánta az odafigyelést, hogy CSAK olyan adatokkal dolgozzak, amelyekkel nem követek el jogsértést. A törvény szürke foltjait kihasználva valósulhatott meg ez a kutatás. Az alábbi törvények problémát okoztak, de nem vonatkoznak erre a dolgozatra, mivel csak publikusan elérhető adatokat nyertem ki, a megszerzett információt nem tettem közzé, a személyes adatvédelmet tiszteletben tartottam, nem használtam ki informatikai rendszereket, és az információt nem használtam fel haszonszerzés céljából:

- Btk. 219. § Személyes adattal visszaélés
- Btk. 373. § Csalás
- Btk. 423 § Információs rendszer vagy adat megsértése

Ezzel szemben joghézagot találtam a BTK-ban:

„A Magyar Büntető Törvénykönyv (Btk.) nem tartalmaz külön bűncselekményt, amely személyazonossággal való visszaélésre vonatkozik, azonban az ilyen cselekmények számos más bűncselekményhez vezethetnek (pl. csalás, információs rendszer elleni csalás, személyes adatok jogosulatlan felhasználása, okmányhamisítás, közokirat-hamisítás, pénzforgalmi eszközök jogosulatlan használata).” [6]

Ezeket az eredményeket alapul véve lehetőségeket teremt a további kutatások és intézkedések számára az egyetemi és jogi közösség és folyamatok fejlesztésére.

## 6. Összefoglalás

A kutatás folyása közben nagyon sokat tanultam a social engineeringről, a jogi háttéréről, és (sajnos) könnyed alkalmazásáról. Tapasztaltam az etikus hackelés 5 fázisát, az emberi naivitás hátrányait, de a legfontosabb, amit tanultam, hogy az emberek túlnyomó része nem elég körültekintő, nincs felkészülve egy ilyen jellegű támadásra.

Az AI által alkalmazott social engineering technikák és pszichológiai hadviselés alapelvei alátámasztják, hogy a technológia milyen mértékben képes utánozni és kihasználni az emberi viselkedést az online térben, milyen játszi könnyedséggel alkalmazhatja olyan ember is, aki manuálisan viszi fel az adatokat és nem is kompetens az ilyen jellegű támadások kivitelezésében.

### 6.1., „Si vis pacem, para bellum”

**Ha békét szeretnél, készülj a háborúra.** A 21. század kiberbiztonsági kihívásai azt követelik meg, hogy az oktatási intézmények erősítsék meg kiberbiztonsági prevenciós intézkedéseiket. Az oktatási rendszereknek hatékony kiberbiztonsági oktatásokat kell nyújtaniuk és innovatív technológiákat kell bevezetniük az adat és személyvédelem erősítése érdekében.

A hallgatók körében kialakított kiberbiztonsági oktatások segítik a digitális fenyegetések tudatosabb kezelését. Az autentikáció valós térbe helyezése jelentősen hozzájárulhat a digitális identitások megerősítéséhez és a kiberbiztonság javításához.

## 7. Köszönetnyilvánítás

Elsősorban szeretném megköszönni Gyurák Gábor tanár úr motivációját, fáradhatatlan munkáját és belém fektetett bizalmát, hogy ez a projekt elkészülhessen. Rendkívül sokat tanultam a feladatból, amit a jövőben tudok kamatoztatni a jó cél érdekében.

Szeretnék emellett köszönetet nyilvánítani kedves páromnak és hallgatótársaimnak, akik „kooperáltak” a projekt elkészültében. Leginkább elviseltek amíg a dolgozat elkészült.

Végül de nem utolsó sorban, szeretném megköszönni a jogászbarátaimnak, akik szakmai kompetenciájukkal segítettek meghúzni projektem legális határait.

## 8. Irodalomjegyzék

ESET:

<https://www.eset.com/hu/it-biztonsagi-temak-cegeknek/social-engineering/>

VERIZON 2020 Adatbiztonsági Vizsgálati Jelentés:

<https://www.verizon.com/about/news/verizon-2020-data-breach-investigations-report>

MASLOW, A. H. (1968):

Cím: "*Toward a psychology of being.*"

Helyszín: New York: D. Van Nostrand Company.

MAGYAR KÖZÖSSÉGI MÉDIA KÖRKÉP:

<https://www.researchcenter.hu/cikkek/magyar-kozossegi-media-korkep/>

EAGLY, A. H., & CROWLEY, M. (1986)

Cím: "*Women receive more help than men from same-sex and cross-sex dyads*"

Folyóirat: Journal of Personality and Social Psychology, 50(6), 1310-1315.

YEH, C. H., CHENG, C. Y., & CHEN, C. J. (2015):

Cím: "*The impact of personality traits and leadership styles on innovation capability of information technology teams. Journal of Vocational Behavior.*"

Folyóirat: Journal of Vocational Behavior, 86, 115-125.

TÓTH, D. (2020):

Cím: "*Azonosítási bűncselekmények a Darkneten és a közösségi médiában.*"

Folyóirat: Jogtudományi Közlöny, 75(11), 428-441.

<https://ujbtk.hu/david-toth-identity-crimes-on-the-darknet-and-the-social-media/>

## 9. Nyilatkozat

Alulírott, Tolnai Máté Gergely, a Tudományos Diákköri dolgozat készítője, aláírásával nyilatkozik, hogy a következők igazak és érvényesek a saját Tudományos Diákköri dolgozatára:

A jelen dolgozat teljes egészében és kizárólag az alulírott munkája, saját gondolatai és kutatási eredményei alapján készült.

A felhasznált irodalmi forrásokat teljes körültekintéssel és tisztességes módon kezelte, megfelelően hivatkozott rájuk a dolgozat megfelelő részeiben, és elkerülte a plágiumot.

A munkája során minden vonatkozó jogszabályt, egyetemi irányelvet és etikai szabályt betartott.

Ezen nyilatkozattal az alulírott kijelenti, hogy a Tudományos Diákköri dolgozat a saját eredeti munkája, és semmilyen módon nem sérti mások szellemi tulajdonjogait vagy etikai normáit.

Dátum:

Aláírás: \_\_\_\_\_

Tolnai Máté Gergely