NE HAGYD MAGAD BECSAPNI!

Szerzők:

Ildikó Pšenáková (PhD)
Trnavská univerzita v Trnave (Szlovákia)

Szerző e-mail címe:
ildiko.psenakova@gmail.com

Lektorok:

Szabó Tibor (PhD)
Univerzita Konštantína Filozofa v Nitre (Szlovákia)

Peter Pšenák (Ing)
E-group Ltd.

…és további két anonim lektor

Absztrakt

A számítógép-biztonsága és a rajtuk tárolt adatok védelme napjaink egyik legnagyobb problémái közé tartoznak, mivel az internet és az infokommunikációs rendszerek lehetőséget adnak a számítógépes támadásoknak. De léteznek nem technikai jellegű támadások is, amikor a támadó pszichológiai manipuláció útján akar információt szerezni. Számos formája lehet (személyes kapcsolat, telefon, e-mail), a lényege ugyanaz, emberek becsapásával minden jog és engedély nélkül a támadó személy bizalmas adatokhoz akar jutni.

Kulcsszavak: pszichológiai manipuláció, adat halászat, védelem, oktatás

Diszciplína: informatika, oktatás

Abstract

DO NOT BE FOOLED!

Computer security and the protection of data stored on computer devices is one of the biggest issues today, as the Internet and info-communicational systems allow for different cyber-attacks. But there are also attacks of a non-technological nature when an attacker seeks information through psychological manipulation. It can take many forms (personal contact, phone, e-mail etc.) however it is trying to achieve the same outcome, to trick people into getting confidential information without any rights and permissions.

Keywords: social engineering, phishing, protection, education

Disciplines: informatics, education

Pšenáková, Ildikó (2020): Ne hagyd magad becsapni! *Lélektan és hadviselés – interdiszciplináris folyóirat*, II. évf. 2020/1. szám. 55-65. doi: 10.35404/LH.2020.1.55

A jelenlegi helyzet

Ma már szinte természetes, hogy nagyon sok munkahelyen úgy indul a mindennapi munka, hogy az ember megnézi a beérkezett postáját. De nem csak, vagy inkább nem is csak az asztalon heverő borítékokat, hanem a számítógépen, mobilján, vagy más elektronikus eszközén érkezett elektronikus leveleket (e-mail) böngészi át. Sajnos, a felhasználók egyre gyakrabban találnak közöttük olyanokat is, amelyek tartalma fenyegető és rosszindulatú szándékkal lett továbbítva.

```
_________
   Tárgy: Harmadik felek férnek
hozzá az eszközéhez. Értesítse a
biztonsági szolgálatot.
   2020. 1. 13-án 15:54kor a
mais@truni.sk írta:

   Helló!
   Mint talán észrevetted, ezt az
e-mailt saját e-mail fiókodról
küldtem neked. Ez azt jelenti, hogy
teljes hozzáféréssel rendelkezem a
készülékéhez.
   Hónapok óta követem téged. A
helyzet az, hogy a géped rosszindu-
latú szoftverekkel fertőzött felnőtt
webhely keresztül, amelyet meglátо-
gatott.
   Ha nem ismeri ezt, magyarázatot
adok. A trójai ló vírus teljes hoz-
záférést és ellenőrzést biztosít
számomra számítógép vagy bármely
más eszközre. Ez azt jelenti, hogy
mindent megnézek a képernyőn, bekap-
csolom a kamerát, és mikrofont, de
te nem tud róla.
   Hozzáférhetek az összes névjegy-
éhez, társadalmi adataihoz, hálóza-
tok és minden levelezés.
_________
```

A levélben észrevehető helyesírási hibák lehetnek, esetleg nem teljesen jó a magyar nyelvezete, sajnos, ezt sokan az ijesztő tartalom olvasása közben nem is veszik észre. Pedig ez a tény, már utalhat arra, hogy a levél becsapás. Legtöbb esetben a levél végén fel vannak tüntetve a lehetőségek, hogyan lehet „megoldani" a problémát. A támadók szinte mindig pénzt követelnek a vírus törléséért, ami még nagyobb átverés, mert, ha a felhasználó át is utalja a pénzt vagy esetleg a bitcoint, akkor sem „tűnik el a támadás", illetve nem is kell eltűnnie, mivel sokszor nem is létezett.

```
_________
Tisztelt nyertesünk!

Örömmel értesítjük, hogy az inter-
netes sorsoláson idén Önnek kedve-
zett a szerencse és megnyerte az 10
milliós fő díjat. A nyeremény kifi-
zetéséhez töltse ki a következő lin-
ken levő on-line kérdőívet…
_________
```

Sajnos, az ilyen típusú leveleknek is sokszor „bedőlnek" a laikus felhasználók. Kitöltik a kérdőívet, amelyben megadják például a bankszámlájuk, személyigazolványuk adatait, és így bizalmas információkhoz jut a támadó személy.

Az ilyen és hasonló támadások az emberi természet tulajdonságait próbálják kihasználni. A támadó nem a technológiai eszközök sebezhetőségét használja ki a támadás során, hanem az emberi befolyásolhatóságot. Ezek

az emberi bizalomra épülő támadások, amelyekre (informatikai szövegkörnyezetben, nem jó indulatú adathalászat jellegű kontextusban) a *Social Engineering*, illetve a magyar megfelelője *pszichológiai manipuláció* vagy *pszichológiai befolyásolás* megnevezés használatos.

Mi a „Social Engineering"?

A Social Engineering támadásoknál a támadó bizalmi kapcsolatot alakít ki az áldozattal, azzal a céllal, hogy később ezt a bizalmat kihasználva, személyes, bizalmas, titkos információkat szerezzen. Az áldozat sok esetben nem is tudja, hogy őt támadás érte. A pszichológiai manipuláció általában az emberi természet két aspektusát igyekezik kihasználni:

1) a legtöbb ember segítőkész és igyekszik segíteni annak, aki segítséget kér,

2) az emberek általában konfliktuskerülők, és inkább együttműködnek, mint nem (Net1).

A pszichológiai manipuláció talán legismertebb és legmegfelelőbb definíciója (Mitnick, 2003): *„A social engineering a befolyásolás és a rábeszélés eszközével megtéveszti az embereket, manipulálja, vagy meggyőzi őket, hogy a social engineer (adathalász) tényleg az, akinek mondja magát. Ennek eredményeként a social engineer – technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni."*

A Social Engineering technikái közé tartoznak például:

- Phishing (Adathalászat)
- Spear phishing (Szigonyozás)
- SMiShing (SMS-alapú adathalászat)
- Vishing (Hangposta alapú adathalászat)
- Pharming (Átirányítás hamisított weblapra)
- Spoofing (Becsapás)
- Typosquatting (URL-eltérítés)
- Whaling (Bálnavadászat)
- Dumpster diving (Kuka búvárkodás)
- Pretexting (Személyiség felvétel)
- Eavesdropping (Hallgatózás)
- Shoulder surfing („Vállszörfözés")

A Social Engineering „támadó" módszerei

Milyen módszereket használ ki a támadó (akire adathalász – social engineer – néven utalhatunk, de a laikus felhasználók gyakrabban használják a hacker szót, amely inkább ismertebb, de a szakmabeliek között egészen mást jelent)?

Ahhoz, hogy védekezni tudjunk a támadások ellen, elsősorban ismernünk kell azok fajtáit.

Phishing - az *adathalászat*: a személyes adatok visszaélés céljából történő gyűjtésének egyik leggyakoribb módja. Az áldozatok becsapásához a támadók az Internetet használják eszközként. A támadások legegyszerűbb módja az e-mail, amelyben a támadó különféle ürügyeket használ. Például: a bank értesíti ügyfelét, hogy a számlája lejár és a meghosszabbításhoz adja meg a banki személyazonosító információkat (hitelkártya számot vagy internetes banki hozzáférési kódokat). Az adathalász e-mailek olyan személyek e-mail címeiről érkeznek, akiket a felhasználó ismer, megbízik bennük és/vagy esetleg a munkahelyi felettese. Az adathalász e-maileket egyszerre több e-mail címre küldik el, azzal az elvárással, hogy valaki „bedől" az e-mailben szereplő információknak, és nyilvánosságra hozza személyes adatait. Az adathalászat szö-

veges üzenetben (SMS) vagy telefonon is megtörténhet.

Az adathalászat célja érzékeny személyes adatok (cím, születési idő, társadalombiztosítási szám, hitelkártya-adatok) beszerzése, bejelentkezési adatok megszerzése az áldozat információs rendszereihez, rosszindulatú alkalmazások telepítése a számítógépre vagy mobiltelefonra. Sikeres támadás után a támadó szinte bármilyen tevékenységet elvégezhet a számítógépen a felhasználó tudta nélkül. Például: a felhasználó fájljainak megsemmisítése vagy titkosítása, fizetés a felhasználó bankszámlájáról, rosszindulatú tevékenységek végrehajtása az áldozat IP-címéről (SPAM, behatolási kísérletek), vírusok terjesztése (az interneten és a helyi hálózaton keresztül).

Egyes források szerint a phishing szó a *password harvesting fishing* angol szavak összevonásából alakult ki, de sokan ezt inkább utólagos belemagyarázásnak tartják. Az adathalászat története pedig kb. az 1990-es évek közepén kezdődött, amikor egy támadó az Amerika Online belső embereként bemutatkozva üzenetet küldött a potenciális áldozatoknak, hogy adják meg jelszavukat az azonosításukhoz, vagy a számlájuk ellenőrzéséhez. A megszerzett jelszavakat egy hacker hírcsatornán közzé is tette (Net2).

Az ilyen fajta támadásokat tapasztalt bűnözők vezetik, gyakran egész bűnözői csoportok rejlenek mögöttük, vagy: akár egész államok is.

Spear phishing – *szigonyozás,* de találkozhatunk a *lándzsás adathalászat,* fordítással is. Míg az „adathalász" tömeges e-mailt használ, a „szigonyos" célokat és nagyon kevés címzettet használ. Az e-mail feladó adatai hamisak lehetnek, de úgy tűnik, hogy megbízható forrásból, például banktól, a vállalat belső informatikai részlegétől, belső alkalmazottól vagy üzleti partnerétől származik. Az üzenet általában felhasználónevet és jelszót igényel, hivatkozást tartalmaz egy webhelyre, ahol a látogatók személyes információkat adhatnak meg, de vírust, trójai falovat, vagy kémprogramokat hordozó mellékleteket is tartalmazhat.

SMiShing – SMS-alapú adathalászat – során a támadó a mobiltelefonokon lévő szöveges üzeneteket (SMS: Short Message Service) használ arra, hogy megpróbálja rávenni az áldozatát, hogy elárulja személyes adatait. A szöveges üzenet olyan webhelyre vagy telefonszámra mutató hivatkozást tartalmazhat, amely automatikusan a hangválasz-rendszerhez kapcsolódik.

Vishing – adathalászat telefonon keresztül. Például a Voice over IP (VoIP) technológia segítségével, amely lehetőséget ad meghamisítani a hívóazonosítót. Lényege, hogy a támadó valamilyen hangátviteli technológiát használ. Mivel az emberek többsége bízik a telefonos hálózatokban, nem feltételezi, hogy a hangüzenet nem hiteles helyről érkezett. A csaló általában úgy tesz, mintha egy törvényes üzletkötő lenne, például nyereséges üzletet kínál és általában hitelkártya információt, esetleg más *személyiség lopásra* alkalmas információt igyekszik ezzel a módszerrel megszerezni.

A *pharming* lényege, hogy a támadó a megtévesztett felhasználót tudta nélkül egy hamis, de a megbízhatóhoz nagyon hasonlító weblapra irányítja. Az átirányítás valamilyen rosszindulatú szoftver vagy kémszoftver segítségével történik. A hacker az általa létre-

hozott hamis weboldalon kérdéseket tesz fel, a felhasználó válaszai pedig lehetőséget adnak neki bizalmas, fontos információk megszerzésére és azok rögzítésére.

Spoofing: hamisítást vagy csalást jelent. Az Interneten többféle formája lehet, például a felhasználó e-mail címének hamisítása, hamis weboldal létrehozása. Leggyakoribb a pénzügyi szolgáltatási weboldalak hamisítása, mert ha a támadónak sikerül ellopnia a személyes információkat (jelszavakat, számlaszámokat) a becsapott emberektől, sok pénzhez juthat.

Typosquatting más néven URL-eltérítés: a felhasználó gépelési hibáit használja ki, amikor egy webhely-címet írnak be egy böngészőbe. Ha a felhasználó véletlenül rossz webcímet ad meg, vagy kihagy egy betűt a címből, alternatív weboldalra irányítja, amelyet rosszindulatú célokra szolgál.

> Gyakori hiba, hogy a .COM helyett a címben .OM íródik. Ez Omán országkódja a Közel-Keleten.
>
> Az .OM webhelyek bizonyultak a legveszélyesebb átirányítási helynek.

Az alternatív oldal grafikai dizájnja, amelyre a felhasználó át lett irányítva, első pillantásra nehezen különböztethető meg a érintett intézmények által használt eredetiktől.

A *whaling – bálnavadászat* cégvezetőkre („bálnákra") irányul. Olyan átverés, amelyben az adathalászok megtalálják a társaság legfontosabb ügyvezetőjének vagy vezetőjének nevét és e-mail címét (ezek az információk legtöbb esetben szabadon hozzáférhetőek a cég weboldalán), és e-mailt készítenek a társaságban betöltött szerepükre vonatkozóan. Az e-mail tartalma megpróbálja rávenni a vezetőket, hogy üssenek egy billentyűre, vagy kattintsanak egy linkre, amely olyan webhelyre irányít, amelyről rosszindulatú szoftverek töltődnek le a gépükre. De az e-mail szövegének hatására érzékeny információkat vagy vállalati titkokat is közzé tehetnek a hiszékeny vezetők.

Dumpster diving – kuka búvárkodás: a támadó kereskedelmi vagy lakossági szemét tárolókban keresgél, azzal a céllal, hogy olyan információkat szerezzen, amelyek alapján csalást vagy lopást lehet elkövetni. Az emberek sokszor úgy gondolják, hogy ami a szemetesbe került, az már meg is semmisült és gyakran értékes információt dobnak ki felelőtlenül a szemétbe. A támadónak nincs más dolga, csak a megfelelő szemetesben keresgélni. Ezért érdemes és sokszor kötelező szétnyúzni, elégetni, iratmegsemmisítő berendezéssel ledarálni, egyszóval megsemmisíteni az érzékeny, fontos, titkos, de már felesleges dokumentumokat.

A *baiting* az emberek kíváncsiságán alapszik. A támadó valamilyen hordozható adathordozót (CD, DVD, pendrive, memóriakártya), vagy akár veszélyes tartalommal ellátott mobil telefont (ezek a „csalik") valahol látható helyen otthagy (célszerűen egy számítógép közelében). A figyelemfelkeltés érdekében az ilyen tárgyakon gyakran „érdekes" szöveg található, pl.: „szexi képek", „bizalmas", stb. Az arra elhaladó személy azt gondolja, hogy találta. A talált tárgyon azonban rosszindulatú szoftverek rejlenek, és amikor a gyanútlan áldozat az eszközt csatlakoztatja a számító-

géphez, hogy megtudja, hogy az kié lehet vagy mi annak a tartalma, akkor bekövetkezik a fertőzés.

De megtörténhet ez az online világban is. Gyakori eset a kalózszoftverek használata folyamán történő fertőzés. Az ingyen letölthető szoftverek vonzóak, és csalogatják a felhasználókat, de letöltés után megfertőzik a számítógépet. A telepített víruskereső szoftver gyakran jelezheti, hogy rosszindulatú kódot talált a kalóz szoftverben, de ezt a felhasználók nem mindig veszik figyelembe. Ezzel meg is történik a baj, a kártékony szoftverek információkat küldenek a felhasználók tevékenységeiről, jellemzően érzékeny információkat, például bankszámlaszámot, jelszót, vállalati hozzáférési információkat, fizetési kártyaszámot, stb.

Pretexting: olyan támadásforma, amellyel a támadók nyílt forrásból vagy adathalászattal előzetesen felkészülnek az áldozatokkal kapcsolatos információkból és így próbálnak meg általában telefonon még több információhoz jutni. (Bodó és tsai., 2018)

Eavesdropping – hallgatózás: a beszélgetések jogosulatlan lehallgatása. Ha két fél beszélgetését akár négyszemközt, akár telefonon illetéktelen harmadik személy lehallgatja, sokszor fontos adatokat gyűjthet. Ha számítógéppel történik a lehallgatás, akkor a támadó kihasználja a nem biztonságos hálózati kommunikáció hátrányait a küldött és fogadott adatok eléréséhez. Az ilyen támadásokat nehéz felismerni, mert a hálózati átvitelben nem okoznak rendellenes működést. Ha személy hallgatózik, akkor megpróbál elrejtőzni is.

A *shoulder surfing* – „váll szörfözés" kedvelt technikája a PIN-kód vagy jelszó megszerzésének. A támadó nem kerül közvetlen kapcsolatba az áldozattal, hanem a támadó közel kerül hozzá, elhelyezkedik mögötte, és az áldozat *válla felett* közvetlenül megfigyeli, amikor az a karaktereket leüti a billentyűzeten. Közben úgy tesz, mintha nem is nézne oda. A leggyakoribb esetek a PIN kódok, beléptető rendszerek, kaputelefonok kódjai, hívókártyák, hitelkártyaszámok, stb. Gyakori a pénzkiadó automatáknál, hogy valamilyen szerkezet, távcső vagy kamera felhasználásával igyekeznek megszerezni a PIN kódot.

A legegyszerűbb védekezés a leselkedők ellen, ha vigyázunk arra ki áll mögöttünk és a kódok bevitelekor eltakarjuk a konzolt.

Végezetül nem lehet figyelmen kívül hagyni azt a tényt sem, hogy az adathalászat eredménye általában valamilyen olyan információ, melyet más jellegű, technikai támadások kivitelezéséhez lehet felhasználni. Az ilyen támadások azonban már jelentős kárt okozhatnak a felhasználóknak és a szervezetnek is (Oroszi, 2015).

Az összes említett adathalász fajta emberi manipulációt alkalmaz, ezért technikai intézkedésekkel nehéz ellenük védekezni. A leghatékonyabb védelem a tudatosság növelése és a hatékony adatvédelmi viselkedés kialakítása lehet.

„A gyakorlatban még nagyon sok más veszély és támadás is létezik, és folyamatosan újak és újabbak látnak napvilágot. Ezért is nagyon fontos, hogy ez a problémakör teret kapjon az oktatásban" – írja Pšenáková és Szabó (2017).

A Social Engineering elleni védekezés lehetőségei

Az előzőek alapján joggal merülhet fel a kérdés, hogy miként védekezhetünk az adathalászat ellen? A legfontosabb védelem mindenekelőtt az emberek óvatossága.

Az adathalász típusú támadások sikere főként a kiszemelt felhasználó döntésein múlik. Ezért a védelem leggyengébb láncszeme a felhasználó, mivel az ő naivitása („gyenge" jelszavak), sokszor gondatlansága (felügyelet nélkül hagyott működő számítógép), ismerethiánya (hiányzik a védelemhez szükséges tudása) csökkenti a rendszer biztonságosságát (Pšenáková, 2017).

A kevésbé szakképzett felhasználó számára igazán könnyen alkalmazható módszer talán nincs is, de a „Legyünk óvatosak!" gondolat szem előtt tartása segíthet. A védekezés alapja azonban az, hogy a felhasználónak tudnia kell, mi ellen kell védekeznie, milyen veszélyekkel kell szembe néznie. A gyakorlatban nem találunk egy univerzális módszert, amely minden esetben tökéletes védelmet nyújtana. De léteznek általános elvek, melyek betartásával minimálisra csökkenthető a támadás kockázata (Pšenáková és Szabó, 2017).

A védelem legjobb módja az éberség a személyes és elektronikus kommunikációban is. Néhány általános elv, vagy tanács:

- Ne adjunk bizalmas információkat olyan személyeknek, akiknek személyazonosságát nem ismerjük!
- Személyes adatot lehetőleg ne adjunk ki senkinek elektronikus levélben vagy weblapon!
- Soha ne adjunk meg bejelentkezési információkat, például felhasználóneveket, jelszavakat vagy más azonosítási módszereket a munkahelyen, de még a magánszféránkból sem!
- Ha látszólag hiteles és legitim forrásból származó támadó e-mailben vagy telefonon bizalmas információkat (jelszavak, dokumentumok küldése...) kér, ellenőrizzük a forrás hitelességét!
- Olyan érzékeny információkat, amelyekre már nincs szükség, de amelyek mégis kárt okozhatnak a cégnek vagy személynek, semmisítsünk meg!
- A talált adathordozót jobb, ha nem használjuk, vagy használat előtt gondosan ellenőrizzük a tartalmát!

Összegezve a felhasználóknak tisztában kellene lennie bizonyos szabályokkal, melyek betartásával sok felesleges gond és probléma megelőzhető. Megoldás lehet a megfelelő oktatás, mely felkészíti a felhasználót az ilyen helyzetekben való helyes eljárásokra. Természetesen az oktatás sem garantálhatja teljes mértékben a veszély elhárítását, de mindenképpen nagy előrelépést jelenthet.

Hol tart az oktatás?

A számítógép felhasználók többségét a számítástechnikában kevésbé járatos felhasználók közé sorolhatjuk, ezért nem ismerik a veszélyforrásokat és a lehetséges védekezési módokat sem. Gyakran azt hiszik, hogy a technikai eszközök és tűzfalak ellenállnak a támadóknak és a védelem áttörhetetlen. Közben megfeledkeznek egy lényeges biztonságtechnikai tényezőről az emberi tényezőről. Ha támadás éri a számítógéprendszert az emberek viselkedése sokszor kiszámíthatatlan, és gyakran a probléma növekedését idézi

elő. Ezért szinte elengedhetetlen, hogy elsajátítsák legalább a legszükségesebb tudást és megfelelő készségeket, hogy kellőképpen biztosítsák saját és mások számítógépes rendszereit.

Szlovákiában az informatika oktatása már az általános iskola alsó tagozatán kezdődik. Az erre „szolgáló" tantárgy az „Informatikai nevelés" megnevezést kapta, később „Informatika" néven fut tovább az oktatás és a diákoknak lehetőségük van érettségi vizsgát is tenni belőle. De ma a tanulók és diákok más tantárgyakon is találkoznak az infokommunikációs eszközökkel, mivel a tanárok szinte rendszeresen használják azokat az oktatásban és természetesen maguk a diákok a tanulásban. Az informatika oktatása így folyamatosan épül fel és lehetőséget ad megismertetni a számítógép használatával járó kockázatok, támadások ismertetésére és a szükséges védelemi jártasságok elsajátítására. Ehhez azonban elsősorban a pedagógusoknak kell elsajátítani a számítógép biztonságos használatát. Ezért is szükséges és indokolt a számítógépes biztonság oktatása a már gyakorló pedagógusoknak, és elsősorban a leendő informatika tanároknak.

Jelen tanulmány szerzője a 2017. évben megjelent több cikkben még arról írt, hogy „A rosszindulatú szoftverek és a pszichológiai manipuláció elleni védelem, és a számítógép biztonságos használatának oktatására a leendő pedagógusok számára az egyetemeinken a jelenleg akkreditált tantervekben nincs külön tantárgy. Sajnos, még a leendő informatika tanárok képzésében sincs erre a témakörre irányuló tantárgy" (Pšenáková, 2017). Örömmel mondhatjuk, hogy 2019-ben már a Nagyszombati Egyetem Pedagógiai Karán változott a helyzet. Ez elsősorban „Az informatika, mint a tudásalapú gazdaság fejlesztésének eszköze" projektnek köszönhető. A projekt keretein belül, sikerült elkészíteni egy 12 tanórás tantárgyat, melynek címe: „Informačná bezpečnosť" (Információbiztonság).

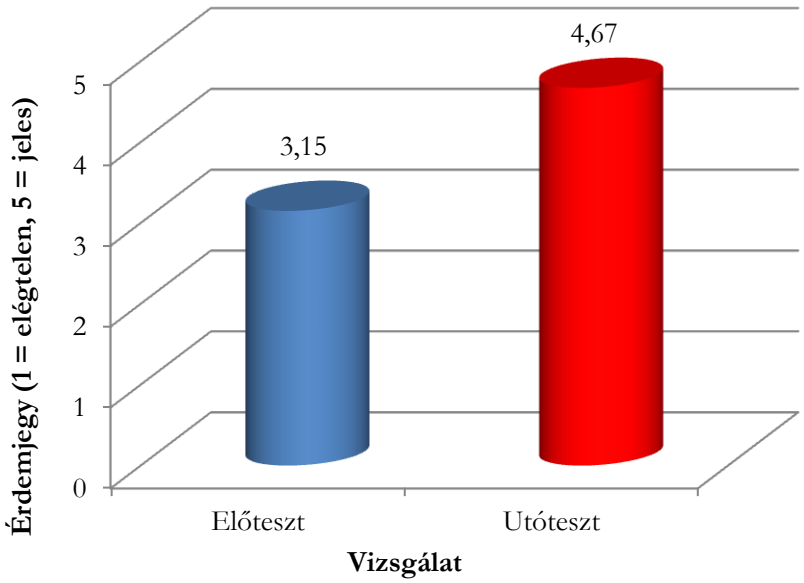
Az oktatás a 2019/2020 tanév első félévében kezdődött. A tantárgyat 23 leendő pedagógus (hallgató) látogatta. Mindegyikük szakpárosítása az informatikát is tartalmazta.

A projekt igényeinek megfelelően az oktatás előtt és után felmértük a hallgatóink tudását az adott témakörről. A teszt 16 pontozott, különböző típusú kérdést tartalmazott. A zárt kérdésekben egy vagy több jó választ lehetett megjelölni a felkínált válaszokból.

Mivel feltételeztük, hogy a hallgatók még nem foglalkoztak a témával, nem ismerték a fogalmakat, úgy gondoltuk, hogy ha felkínáljuk a lehetséges választ, válaszokat, sokkal könnyebbnek, egyszerűbbnek érzik a felmérést és logikus következtetés alapján megtalálják a megoldást. Ugyanis nem szerettük volna, ha ez az előtezst elriasztotta volna a hallgatókat – hanem épp ellenkezőleg: a célunk volt az is, hogy keltsük fel az érdeklődésüket, tudatosítsuk bennük az ilyen tantárgy elvégzésének a szükségességét.

Az 1. ábra mutatja be az elő- és az utótesztben elért érdemjegek átlagát (a magyar köznevelésben megszokott ötfokú osztályozási rendszer értékeit használva, ahol 1 = elégtelen, 2 = elégséges = 3 = közepes, 4 = jó, 5 = jeles. Ezt azért célszerű hangsúlyozni, mert Szlovákiában is ötfokú osztályozási rendszer van alkalmazásban, ám ott az 1-es jelenti a jeles osztályzatot). A hallgatók által megszerzett érdemjegyek tekintetében az e-

1. ábra: A felmérések eredménye (forrás: a Szerző)



lőteszt átlaga 3,15 volt, az utóteszté pedig 4,67. A különbség 1,52 – ami arra utal, hogy a hallgatóknak gyarapodott a tudása.

Érdekességként, bemutatunk egy feladatot, amelyiket az előteszt során egyetlen hallgató sem oldott meg helyesen (2. ábra). Az ismételt tesztelésen 12 diák teljesen helyesen és a többiek egy-két hibával oldották meg.

2. ábra: egy példa az alkalmazott feladatokra (forrás: a Szerző)

Kösse össze az öszetartozó bal és jobb oldali kifejezéseket!

Phishing	**Social Engineering**
Remote administration	**Malware**
Vishing	
Rootkit	
Červ (Féreg)	
Hoax	**Spyware**
Keylogger	

Ez a példa is illusztrálja, mennyire hiányos volt a diákok tudása a témakörről, és hogy mekkora mértékben segíthet és segített a tantárgy oktatása, még ilyen viszonylag kevés óraszámban is.

A számítógépes biztonsággal, a rosszindulatú szoftverek és a pszichológiai manipuláció elleni védelemmel kapcsolatos tudás azonban nemcsak az informatika tanárok számára fontos, szükséges lenne az egész pedagógusképzésébe beiktatni a tematikával foglalkozó tantárgyat.

Befejezés

Jelen tanulmányban bemutattuk a leggyakoribb, legismertebb social engineering támadási technikákat és vázoltuk a védekezési módokat. A gyakorlatban azonban még sok más létezik, és folyamatosan újak készülnek. A támadók továbbra is új ötletekkel állnak elő, és új, hatékonyabb rosszindulatú programokat és adathalász technikákat hoznak létre. Ezért is tartjuk nagyon fontosnak, hogy megfelelő helyet találjunk a témával kapcsolatos kérdések taglalására az összes leendő tanár tantervében, és nem csak az informatika tanárok oktatásában.

Ha leendő tanáraink elsajátítják az információs rendszereket érintő különféle támadások veszélyeit, felismerik azokat és tudni fogják a védelem lehetséges módszereit, remélhetőleg sokkal nagyobb figyelmet fordítanak számítógépük biztonságára, az adatok védelmére és nem „hagyják magukat becsapni". Ezt követően, tudásukat tovább adják diákjaiknak, és így hozzájárulnak a jövőbeli sikeres támadások számának csökkentéséhez.

Zárszóként

E tanulmány a COVID-19 (koronavírusbetegség) világjárvány időszakában keletkezett. Sajnos e járván is apropóul szolgált az adathalászok számára. a virtuális világban megjelentek a járványhelyzetet khasználni akaró internetes csalók, adathalászók üzenetei, posztjai, e-mailjeik... Tipikus példa erre a „Coronavirus map", ami azt ígéri, hogy megmutatja a koronavírus terjedését a világon, de valójában egy vírust telepít a számítógépre, mobiltelefonra, és segítségével felhasználóneveket, jelszavakat továbbít a támadónak. A tanulság: a fokozott óvatosság nem csak a reális életben, hanem a virtuális világban is kötelező!

Irodalom

Bodó, A. P., Marsi, T., Sebők, V. és Zámbó, N. (2018). *Célzott kibertámadások*. letöltés: 2020.03.02. Web: https://nkerepo.uninke.hu/xmlui/bitstream/handle/123456789/7229/C%E9lzott%20kibert%E1mad%E1sok.pdf;jsessionid=25A4603DF65BA3DB004257712D1EB942?sequence=1

Mitnick, K. D. és Simon, W. L. (2003). *A legendás hacker – A megtévesztés művészete*, Perfact Kiadó, Budapest.

Net1: *Social Engineering*. letöltés: 2020.02.23. Web: https://sealog.hu/tudastar/fogalomtar/social-engineering

Net2: *Az adathalászatról (phishing, pharming)*. letöltés: 2020.02.02. Web: https://www.cert.hu/az-adathalaszatrol-phishing-pharming

Oroszi, E. (2015). *Social engineering támadási technikák. Avagy a végső megoldás: a felhasználó.* letöltés: 2020.03.02. Web: http://www.securinfo.hu/termekek/it-biztonsag/1295-social-engineering-tamadasi-technikak-avagy-a-vegso-megoldas-a-felhasznalo.html

Pšenáková, I. (2017). Számítógépes biztonság oktatása a leendő tanároknak. In: *A magyar tannyelvű tanítóképző kar 2017-es tudományos konferenciáinak tanulmánygyűjteménye.* Subotica: University of Novi Sad, Hungarian Language Teacher Training Faculty, ISBN 978-86-87095-76-2, 1022-1031

Pšenáková, I. és Szabó, T. (2014). Niektoré aspekty potreby kurzu počítačovej bezpečnosti pre neprofesionálov. In: *Science for Education - Education for Science - II.volume* = Nitra: UKF, p. 311-317

Pšenáková, I. és Szabó, T. (2017). Pedagógusok versus hackerek, vírusok és hasonló férgek. In: *InfoDidact 2017*. Budapest: Webdidaktika az Oktatásért és az Információs Társadalomért Alapítvány. p. 1-11.

Schneck Zs. (2020). *Hazudj, ha tudsz! Social engineering, avagy amikor a felhasználót hackelik.* letöltés: 2020.03.12. Web: https://www.itbusiness.hu/technology/aktualis_lapszam/kiadvanyok/annofuturum-2019/social-engineering-avagy-amikor-a-felhasznalot-hackelik