Tallinna Ülikool

Digitehnoloogiate instituut

Informaatika

ARVUTIKASUTAJATE TEADLIKKUS SOTSIAALMANIPULATSIOONIST TALLINNA ÜLIKOOLI ÜLIÕPILASTE NÄITEL

Bakalaureusetöö

Autor: Siim Karoman

Juhendaja: Kaido Kikkas

Autor: ..... „ ..... „ 2017

Juhendaja: ..... „ ..... „ 2017

Instituudi direktor: ..... „ ..... „ 2017

Tallinn 2017

Autorideklaratsioon

Deklareerin, et käesolev bakalaureusetöö on minu töö tulemus ja seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

.....	.....
(kuupäev)	(autor)

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Siim Karoman (sünnikuupäev: 15.09.1989)

1. annan Tallinna Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose „Arvutikasutajate teadlikkus sotsiaalmanipulatsioonist Tallinna Ülikooli üliõpilaste näitel“, mille juhendaja on Kaido Kikkas, säilitamiseks ja üldsusele kättesaadavaks tegemiseks Tallinna Ülikooli Akadeemilise Raamatukogu repositooriumis.

2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.

3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tallinnas, _____

allkiri ja kuupäev

SISUKORD

SISSEJUHATUS

Sotsiaalmanipulatsioon võib olla paljude inimeste jaoks uus mõiste, kuid muutub tänapäeva infoühiskonnas järjest aktuaalsemaks ja olulisemaks. Inimesed võivad sotsiaalmanipulatsiooni kogeda nii tööelus kui ka vabal ajal. Üsna tavaline on, et internet on olemas ka telefonis ja seetõttu oleme kogu aeg ühendatud ja kättesaadavad. Info hulk on väga suur ja seepärast ei pruugita tähele panna ohukohti, mis internetis varitsevad. Peale selle muutuvad ründajad järjest oskuslikumaks. Tihti võib juhtuda, et kõige suurem turvarisk on inimene ise. Seega peaks veebis käituma vastutustundlikult.

Viimasel ajal räägitakse järjest enam erinevatest petukirjadest või lunavarast. Tänu selliste juhtumite meediakajastustele saab tõsta inimeste teadlikkust, et nad ei langeks enese teadmata rünnakute ohvriks. Kui inimesed teadvustavad endale võimalikud ohud ja riskid, siis on kergem võimalikke rünnakuid vältida.

Töö eesmärk on teada saada, kui teadlikud on Tallinna Ülikooli üliõpilased sotsiaalmanipulatsioonist ja selle võtetest. Uurimuse eesmärgist lähtuvalt otsitakse vastust järgmistele uurimisküsimustele.

- Kas Tallinna Ülikooli üliõpilased teavad, mis on sotsiaalmanipulatsioon?
- Kui teadlikud on üliõpilased sotsiaalmanipulatsiooni võtetest?

Töö koosneb neljast suuremast peatükist. Esimeses peatükis antakse ülevaade sotsiaalmanipulatsioonist üldiselt. Teises peatükis kirjeldatakse sotsiaalmanipulatsiooni põhivõtteid. Seejärel kirjeldatakse võimalikke tegevusi, mida saab teha sotsiaalmanipulatsiooni ennetamiseks. Neljas peatükk keskendub tehtud uuringule. Peatükis kirjeldatakse töös kasutatud metoodikat ja analüüsitakse küsitluse vastuseid. Uuringu viimases alapeatükis tuuakse välja vastused uurimisküsimustele ja analüüsi tulemustest tehtud järeldused.

1 SOTSIAALMANIPULATSIOONI OLEMUS JA TAUST

Peatüki eesmärk on kirjeldada, mis on sotsiaalmanipulatsioon, mis on selle eesmärk ja kuidas seda igapäevaelus kasutatakse.

Social engineering ehk sotsiaalmanipulatsioon on üks kurjategija ründe viisidest, kuidas saada ligi tundlikule infole. Selleks kasutatakse ära inimeste loomust ja selle nõrkasid kohti. Sotsiaalmanipulatsiooni tehnikat kasutatakse, et saada infot ja teadmisi, mille abil oma rünnakut plaanida. Selle asemel, et kasutada keerukaid programme, millega süsteemi otse rünnata, üritab manipulaator saada infot otse inimese käest. Proovitakse ennast esitleda asutuse töötaja, kliendi, ülemuse või mõne muu isikuna, kes on seotud asutuse või selle klientidega. Ründaja proovib saada teada võimalikult palju infot: töötajate nimesid, kasutajaid, serveri nimesid, IP-sid, paroole jne. Peale selle võib ta üritada uurida üldiselt asutuse süsteemi ülesehituse kohta ja selle võimalikke nõrkasid kohti. Asutuse süsteem võib olla väga turvaline ja kindel, aga inimese faktor jääb alati. (Greavu-Şerban & Şerban, 2014.)

Sotsiaalmanipulatsiooni eesmärk on inimesi manipuleerida avaldama infot nii, et nad ise ei saaks arugi, et on avaldanud midagi, mida nad ei tohiks. Neile jääb mulje, et midagi pahatahtlikku ei ole toimunud. Enamasti ei jää see hetk, kui rünnak on toimunud ja info avaldatud, meeldegi, kuna inimeste jaoks midagi kahtlast ei juhtunud ja see oli osa igapäeva tegevustest. (Greavu-Şerban & Şerban, 2014.)

Sotsiaalmanipulatsiooni on hakatud kasutama üha rohkem, sest traditsionaalsete rünnakute efektiivsus on kahanenud. Inimestest sõltumatuid turvasüsteeme on hakatud järjest rohkem kasutama ja need on muutunud tõhusamaks. Ründajad on võtnud tarvitusele alternatiivmeetodid, mis kasutavad ära nii tehnoloogia vead, kui ka inimeste omad. Samuti on probleemiks see, et sotsiaalmanipulatsiooni levikust ei olda veel nii teadlikud. (Janczewaki & Fu, 2010.)

Turvatunne on tihti illusioon, mida võimendab veel kergeusklikkus, naiivsus või ignorantsus. Sotsiaalmanipulatsioon saab toimida siis, kui inimesed ei pööra tähelepanu headele turvakommetele. Paljud IT-firmad on arvamusel, et nad on teinud oma ettevõtte rünnakutele immuunseks, kui nad on võtnud kasutusele standardturvameetmed. Näiteks tulemüür, liikumisandurid ja tugevamad autentimissüsteemid, nagu ajapõhised *token*'id

ja biomeetrilised *smart*-kaardid. Need, kes arvavad, et ainuüksi turvatoodetest piisab täielikuks turvalisuseks, petavad ennast. Varem või hiljem kogevad nad turvavigu. Arendajad parendavad koguaeg turvalisustehnoloogiat ja see teeb järjest raskemaks ründajatel tehnoloogilises pooles nõrkusi leida. Seega pööravad ründajad järjest rohkem tähelepanu inimlikele nõrkustele, mida saaks ära kasutada, sest seda on kergem leida kui nõrkust tulemüüris. (Mitnick & Simon, 2002.)

Ohu hindamisel tuleb kasuks ründaja motivatsiooni teadmine ning tema oskuse tase. Inimene peaks teadma, mis info peaks kindlalt olema kaitstud, et luua süsteemid selle kaitsmiseks. Üldiselt jagunevad ründajad kaheks: professionaalid, kes teenivad raha oma rünnakutega ja amatöörid, kes tahavad tõestada oma oskuski või saada tunnustatud oma tegude kaudu. (AL-Johani & AL-Msloum, 2013.)

Amatöörhäkkerite alla kuuluvad näiteks häkkerid, kes ei tee seda rahalisel või väljapressimise eesmärgil, vaid näiteks niisama huvi pärast või et tekitada pahandust. Nende motivatsioon on näidata oma oskuski ja näidata, et nad saavad seda teha. Siia alla kuuluvad ka aktivistid, kes oma tegevusega võitlevad millegi ideoloogilise või religioosse eest. Enamasti on nad rohkem professionaalid kui amatöörhäkkerid. (AL-Johani & AL-Msloum, 2013.)

Üks suurimaid ajendeid rünnakuteks on rahaline kasu. Ründaja soovib saada lihtsalt rohkem raha või tunneb, et ta väärib rohkem raha. Sellistele eesmärkidele võivad kallutada ka rahalised probleemid. Ajendiks võib olla ka kättemaks. Kätte saab maksta nii inimesele, kui ka kogu asutusele. Näiteks inimene, kes on vallandatud võib tahta maksta oma tööandjale kätte. Ta on firmas töötanud ja teab firmasisest infot ja asjade käiku. Seega on tal lihtsam kahju tekitada. Lisaks võivad aidata tööl oldud ajal saadud tutvused ja sõbrad. (Allen, 2007.)

Enamjaolt on sotsiaalmanipulaatorid hea suhtlemisoskusega. Nad on sarmikad, viisakad ja nendega on lihtne suhelda. Need on omadused, mis aitavad luua usaldust. Kogenud sotsiaalmanipulaator on võimeline saama ligi põhimõtteliselt igale infole kasutades oma strateegiaid ja meetodeid. Tehnikatargad on vaeva näinud, et luua informatsiooni kaitse lahendusi, et minimaliseerida riske, mis kaasnevad arvuti kasutamisega. Nad on aga jätnud suuresti arvestamata suurima vea – inimfaktori. Inimese intellektuaalsusele vaatamata on inimene ikkagi kõige suurem turvarisk. (Mitnick & Simon, 2002.)

Üheks tuntuimaks sotsiaalmanipulaatoriks võib pidada Kevin Mitnicki, kes on raamatute „The Art of Deception“ ja „Ghost in the Wires: My Adventures as the World's Most Wanted Hacker“ autor.

Aastal 1983 oli Mitnick alles üliõpilane, kuid suutis saada sissepääsu ARPANet-i (Interneti eelkäija), mida kasutasid suured korporatsioonid, ülikoolid ja USA sõjavägi. ARPANet-i pääsemine andis talle ligipääsu Pentagoni ja kõikidele kaitseministeeriumi failidele. Mitnick tegelikult mingeid andmeid ei varastanud. See oli pigem võimalus ennast tõestada. Hiljem, kui sellest teada saadi, Mitnick arreteeriti ja ta kandis lühikest karistust noorte kinnipidamisasutuses. See oli tema esimene karistus illegaalselt arvuti süsteemi sissemurdmise eest. Pärast seda oli Mitnick jätkuvalt FBI radaril ja sattus mitmete uurimiste huviorbiiti. (Iozzio, 2008.)

1994. aastal suutis Mitnick, olles üleriigiliselt tagaotsitav, saada aastaks tööle advokaadibüroosse, kus ta esitles ennast Eric Weissi nime all. Mitnick läks oma kuritegude eest siiski lõpuks vangi. Nüüdseks on ta oma karistuse ära kandnud ja töötab edukalt turvanõustajana, kasutades oma varem hangitud teadmisi ja kogemusi. (Mitnick & Simon, 2011.)

2 SOTSIAALMANIPULATSIOONI PÕHIVÕTTED

Praegusel infoühiskonna ajastul on väga palju erinevaid võimalusi, kuidas inimeste käest tundlikku teavet kätte saada. Ühelt poolt võib läheneda inimesele otse, teisalt võib appi võtta digitaalsed vahendid.

Meetodi valik oleneb enamasti ründaja ajast, kannatusest, isiksusest ja järjepidevusest. Samuti tuleb siin mängu petmise oskus. Selleks et süsteemi tungida, peab ründaja leidma viisi, kuidas saada kätte info süsteemi kasutaja käest. Ründaja saab kätte tundliku info või petab/manipuleerib ta tegema midagi, mis tekitab suure turvaaugu süsteemis, mida ründaja saab ära kasutada. Ükski tehnoloogia ei saa sellise tegutsemise eest kaitsta. Sotsiaalmanipulaatorid kasutavad ära töötajaid ja süsteemi kasutajaid, et läbi murda turvasüsteemidest. (Mitnick & Simon, 2002)

Järgnevalt on välja toodud levinumad sotsiaalmanipulatsiooni viisid, mida manipulaatorid kasutavad.

2.1 Vaatlemine

Lihtne vaatlus võib anda palju infot. Vaatluse teel on võimalik tuvastada, kas rünnatav asutus kasutab võtmeid, kaarte või muid lukustusviise. Peale selle on võimalik teada saada, kas asutusel on väljas suitsunurk, kas sinna pääseb ligi ilma, et peaks kuskilt midagi avama või kellelgi mingit dokumenti näitama. Lisaks on võimalik näha, kui suur on asutuseväline turvatase, kas ja kus on kaamerad, kas on valvureid, kas majast väljas asub väliseid seadmeid, nagu elektrikilbid või ventilatsioon. Lihtsa vaatluse abil on veel palju muud võimalik teada saada, eriti kui olla kannatlik ja dokumenteerida oma vaatlusi. (Hadnagy, 2013.)

2.2 Üle õla vaatamine (*shoulder surfing*)

See on oskus saada ligi informatsioonile lihtsalt vaadates kasutaja arvuti ekraani ja jälgides tema tegevust (nt vaadelda mida ja kuhu trükitakse). Seda on võimalik teha aknast sisse vaadates, ukse vahelt või koridorist piiludes või lihtsalt vestlust pealt

kuulates. Inimesed, kes tegelevad tundliku infoga, peavad olema teadlikud oma ümbrusest. Tähele tuleks panna, kes on lähedus ning kes võib kuulata või vaadelda. Parooli trükkimisel tuleks seda võõraste pilkude eest varjata. Inimesed, kes teevad tööd või tegelevad tundliku infoga avalikus kohas, peaksid jälgima, kuhu nende ekraan on suunatud. Tuleks vältida arvuti ekraani suunamist kellegi vaatevälja. (Cyber Security Tips, 2012.)

2.3 Prügikastis tuhnimine (*dumpster diving*)

See tähendab sihtmärgi prügi läbi otsimist. Eesmärk on leida kasulikku infot. Info, mis prügist leitakse, võib olla väga kasulik. Enamus inimesi ei pööra suurt tähelepanu sellele, mis nad kodus ära viskavad: telefoniarved, krediitkaardi andmed, ravimikarbid, pangakaardi või -kontoga seotud paberid, tööga seotud dokumendid jne. Tööl peaks töötajatele selgeks tegema, et prügist on võimalik leida infot, mida saab pahatahtlikult ära kasutada. (Mitnick & Simon, 2002.)

2.4 Sappavõtmine (*tailgating*)

Sappavõtmine tähendab majja sisenemist inimesele järel, kellel on õigused majja sisenemiseks. Asutused võivad investeerida kümneid tuhandeid dollareid uste turvasüsteemidele, mida on võimalik läbida ainult uksekaardi või koodiga. Nii saavutatakse olukord, kus ukse saab avada ainult inimene, kellel on selleks õigus. Selle süsteemi nõrkuseks on, et süsteem ei kontrolli mitu inimest siseneb, kui uks on avatud. Kui üks õigustega inimene avab ukse, siis temale võib järgneda keegi veel, kellel ei ole õigusi ise siseneda. (Ciampa, 2011.) Samuti on inimese loomus ja viisakus siin olulised faktorid. Keegi ei taha teisel nina ees ust kinni lüüa. Kui liigutakse kellegagi koos, siis ikka hoitakse ust enda taga kauem lahti, et järgnev inimene saaks uksest sisse. (Kikkas, 2016.)

2.5 Maskeerimine

Töötaja ei ole ainuke, kelleks ründaja ennast maskeeruda võib. Kulleriks, töömeheks või isegi külaliseks riietamine annab ründajale hea võimaluse, kuidas majja sisse pääseda. Enda kulleriks maskeerimine on suhteliselt lihtne. Lihtsaim viis on lihtsalt tunked osta. Peale selle on võimalik osta ka mõne tuntud kullerfirma riideid. Need on saadaval näiteks e-bays või mõnel muul veebioksjonisaidil. (Jones, 2004.)

Üks tüüpiline tehnika on läheneda sissepääsule raskete kastidega ja loota, et leidub abivalmis inimene, kes ukse avab. Kui töötaja peaks ründajaga rääkima hakkama, siis veenab ründaja töötajat, et tal on vaja sisse pääseda. Alati võib aidata mõne kõrgemal kohal töötava inimese nime mainimine. Samuti võib majja pääsemiseks end remondimeheks riietada. Selleks tuleb hankida endale tunked või mõne teenust pakkuva firma logoga särk. Administraatorile öeldakse, et tuldi telefoni, tualetti vms parandama. Kui võimalik, siis valitakse aeg, kus haldusjuht pole majas. Samuti võib rõhutada, et tegemist on kiireloomulise asjaga. (Jones, 2004.) Sarnaselt eelpool nimetatud tööriietele võib sama mõju olla ka tavalisel helkurvestil.

2.6 Küsimustike kasutamine

Me kõik oleme kindlasti täitnud varem küsimustikke internetis. Enamjaolt on need kellelgi reaalse uurimuse tarvis valmistatud. Kuid leidub ka selliseid, mille eesmärk on pahatahtlik. Küsimustikud võivad sisaldada küsimusi sinu töökoha kohta, selle infrastruktuuri või näiteks turvameetmete kohta. (Cyber Security Tips, 2012.)

2.7 USB-mälupulga mahajätmine

Ründajad võivad kasutada ka USB-mälupulka, et pääseda ligi tundlikule infole, mida talletatakse arvutis või võrgus. Ründaja võib nakatada USB-mälupulga viiruse või Troojaga. Kui mälupulk ühendatakse arvutiga, siis annab see ründajale ligipääsu sisselogimistele, paroolidele ja muule teabele kasutaja arvutis või võrgus, kus kasutaja arvuti on ühendatud. Ründaja võib jätta USB-mälupulga näiteks põrandale või kuhugi arvutite lähedusse. Tavaliselt valitakse koht, kus liigub palju inimesi. Inimene, kes leiab

mälupulga, sisestab tihti selle enda arvutisse, lootuses, et leiab infot, kellele see mälupulk kuuluda võib. (Information Security Office, kuupäev puudub.)

2.8 Veebisaitide ja meili kasutamine

Sotsiaalmeediasse millegi postitamise või mõne postituse kommenteerimisega peaks olema ettevaatlik. Kui info on üles pandud on põhimõtteliselt kõigil võimalus seda lugeda. Hiljem ei pruugi enam olla võimalik seda infot maha võtta või on juba liiga hilja. Mida rohkem infot postitada, seda suurem võimalus on seda rünnaku tegemiseks kuritarvitada. Veebilehti on võimalik ära kasutada mõtlematute inimeste käest tundliku teabe, nagu näiteks meiliaadresside või paroolide, saamiseks. Näiteks võib veebisait pakkuda võimalust osaleda loosimisel või kampaanias. Sait võib paluda sisestada oma meiliaadressi ja parooli. Parool, mis sisestatakse, võib olla sama või sarnane tema muude paroolidega, näiteks töö e-posti aadressi parooliga. (Cyber Security Tips, 2012; Allen, 2007.)

Üks näide interneti kaudu inimeste mõjutamise kohta on *phishing*. Ründaja saadab võltsitud meili, mis sarnaneb mingi firma või panga ametliku e-posti vormiga ja soovib, et te uuendaksite oma andmeid. Peale selle võib kasutada võltsitud veebilehti, mis on tehtud välimuselt võimalikult sarnaseks. Meilis võib olla link http://www.facebook.com, mis tegelikult suunab sind lingi peale vajutades hoopis mingile muule veebilehele, kus kasutaja juba sisestab oma andmed. (Allen, 2007.)

Näiteks on Eestis levinud juhtumid, kus inimestele saadetakse meile, mis sisaldavad manust, mille avamise tagajärjel krüpteeritakse inimese arvuti. Arvuti vabastamiseks tuleb maksta ründajatele lunaraha. Peale selle levisid tuludeklaratsioonide esitamise ajal petukirjad, mille oli näiliselt saatnud Maksu- ja tolliamet, kuid tegelikult oli ründaja eesmärk saada kasutajate isiklikke andmeid. Sellised juhtumid on saanud meediakajastust (Pealtnägija, uudised), mis aitab tõsta inimeste teadlikkust.

2.9 Telefoni teel info saamine

Sotsiaalmanipulaator võib saada infot ka telefoni teel. Helistaja esitleb ennast inimesena, kellel on õigus saada infot. Näiteks võib pettemanöövriks kasutada selle sama asutuse töötaja identiteeti. Helistaja palub kolleegilt abi ja tuge mõne probleemi lahendamiseks. Kõige lihtsam koht alustamiseks on tehniline tugi. Põhjus on väga lihtne – see ongi tehnilise toe töö, pakkuda töötajatele abi. (Allen, 2007.)

Siin on toodud üks näide telefoni teel info saamisest. Suurfirma tegi kampaania, kus pakkus liitumise eest uut telefoni ühe sendi eest. Paljud ostjad peaksid ennem sellise plaaniga liitumist tegema kindlaks, mis täpsemalt plaanis sisaldub, ilma, et hakkaksid kohe uue telefoni pärast liituma. Sotsiaalmanipulaator, kellele meeldis ühe sendi eest pakutav telefon, aga kellele ei meeldinud üldse pakutav plaan, lahendas olukorra omamoodi. (Mitnick & Simon, 2002.)

Ta helistas ühte peoketi elektroonikapoodi ja väitis, et oli mõned päevad varem rääkinud ühe töötajaga plaanist ning pidi temaga uuesti ühendust võtma, kuid unustas tema nime. Ta viis oma jutuga kõne vastuvõtja selleni, et see ütles ühe töötaja nime (William). Seda sama nime kasutades helistas sotsiaalmanipulaator hiljem keti teise firmasse ja esitles end nüüd Williamina. Ta ütles, et tegi ühe inimesega lepingu, kuid neil on telefonide varu otsa saanud. Kuna teises poes, kuhu ta helistas, neid veel oli, siis olidki nemad nõus selle telefoni väljastama. Seega läkski sotsiaalmanipulaator poodi ja talle anti telefon ilma, et ta oleks pidanud tegelikult ühegi plaaniga liituma. (Mitnick & Simon, 2002.)

2.10 Tähtsa juhi identiteedi kasutamine

Rünnaku tegija esitleb ennast kui kõrgemat juhti selles organisatsioonis, kellel on tähtis tähtaeg. Nii saab inimest sundida endale kasulikku infot jagama. Nagu näiteks, millist kaughaldustarkvara nad kasutavad, kuidas seda seadistada, vajalikud sisselogimisandmed serverile ligipääsemiseks jms. Sellise info kättesaamise järel on ründajal võimalik luua ühendus organisatsiooni võrguga. Ründaja võib paar tundi hiljem tagasi helistada ja öelda, et ta on unustanud oma parooli ja paluda see uuesti lähtestada. (Allen, 2007.)

3 SOTSIAALMANIPULATSIOONI VASTUMEETMED

Eelnevalt on kirjeldatud sotsiaalmanipulatsiooni mõiste, selle eesmärk ja põhilised kasutusviisid. Selles peatükis vaadeldakse lähemalt seda, kuidas end sotsiaalmanipulatsiooni rünnakute eest kaitsta ja milliseid vastumeetmeid kasutada.

3.1 Töötajate koolitamine

Esimene samm sotsiaalmanipulatsiooni rünnakute vältimisteks on teada, mis need on ja õppida nende kohta. Teadmised ei pea olema sügavad, nagu näiteks teadmine, kuidas neid ise läbi viia. Pigem peaks omandama teadmised selle kohta, milliseid rünnakuid on olemas ja mis juhtub, kui nende ohvriks langeda. Lisaks on vaja kindlasti teada olulisi tähelepanekuid, mis vihjavad, et tegemist võib olla pahatahtliku tegevusega. (Hadnagy, 2013.)

Oluline on, et see teadmine oleks omandatud juba enne seda, kui rünnak on toimunud, mitte õppida toimunud rünnakust. Hea oleks informeerida oma töötajaid sotsiaalmanipulatsiooni uutest teemadest. Näiteks võib lugeda mingit raamatut sel teemal, näidata õppevideoid või kutsuda spetsialistid pidama õppekoosolekuid. Põhimõtteliselt võib öelda, et mida rohkem sa tead sotsiaalmanipulatsioonist, seda kergem on ära tunda võimalikke rünnakuid. (Hadnagy, 2013.)

3.2 Info väärtuse hindamine

Üks hea soovitus on see: ole teadlik info väärtusest, mida sul võidakse paluda avaldada. Enne kui edastad informatsiooni, mõtle, kas see inimene peaks seda üldse teadma. Inimestel on sisse ehitatud tahe aidata hädasolijaid. See on üks viise, mida kasutatakse inimeste manipuleerimiseks. Töötaja peaks teadma ja suutma aru saada, kas tegelikult on vaja avaldada sellist infot. Ka kõige väiksemad infokillud võivad aidata kaasa rünnakule. Kui küsimused äratavad kahtlust on üks lihtsamaid viise öelda lihtsalt, et „Vabandust, ma ei või seda infot avaldada“ või lihtsalt öelda, et te ei tea täpselt selle kohta ja suunata nad edasi üldinfosse. (Hadnagy, 2013.)

Töötajate jaoks on hea luua nn stsenaarium. See tähendab, et luuakse küsimustikud või käitumisviisid, mida saab teatud olukordades kasutada. Näiteks kui keegi helistab ja väidab, et on mingi osakonna juht või on administraator, siis tuleks küsida, kas inimese ID-d või muud sellist identifitseerimise võimalust. (Hadnagy, 2013.)

3.3 Andmete klassifikatsioonid

Iga ettevõtte peaks reguleerima andmete väljastamist. Ettevõtte infovarade kaitsmiseks on vaja paika panna andmete klassifikatsiooni poliitika. See poliitika loob raamistiku, tänu millele on töötajad teadlikud andmete tundlikkuse tasemest. Kui neid eeskirju pole, siis peavad suurema osa otsuseid tegema töötajad ise. Töötajate otsused põhinevad enamasti pigem subjektiivsetel aspektidel kui teabe väärtusel. (Mitnick & Simon, 2002.)

Andmete klassifikatsiooni poliitika paneb paika kindlad juhised, mille abil antakse väärtuslikule informatsioonile üks kindel tase. Pärast seda saavad töötajad juba jälgida kindlaid andmete käsitlemise protseduure, et kaitsta ettevõtet hooletu väärtusliku info avalikustamise eest. Juhatus peab paika panema ka info omaniku. Info omanik vastutab väärtuslikud info kaitse eest, otsustab, milline klassifikatsioonitase määrata, vaatab infole määratud tasemeid aeg-ajalt üle ja vajaduse korral uuendab neid. (Mitnick & Simon, 2002.)

Kõige üldisemalt võib andmed jagada nelja kategooriasse: konfidentsiaalne, privaatne, sisemine, avalik. Konfidentsiaalne kategooria sisaldab kõige tundlikumat teavet. Seda ei tohi mitte mingil juhul ettevõttest välja anda ja enamasti teavad sellest ainult teatud inimesed. Privaatse kategooria alla kuuluvad andmed, mis on isiklikku laadi ja mida tohib kasutada ainult asutuse sees (nt töötajate haiguslood, palga või pangakonto info). Sisemine kategooria hõlmab andmeid, mida võib vabalt jagada kõigi ettevõtte töötajatega. Avaliku info alla kuulub teave, mis on loodud spetsiaalselt asutuse väliseks kasutamiseks. Siia alla kuuluvad pressiteated, tootevoldikud jms. (Mitnick & Simon, 2002.)

Peale andmete klassifikatsiooni on veel oluline teada, kuidas tundlikku infot hävitada. Tähtsad dokumendid ja tundlik info tuleks ära viskamise asemele purustada ja muuta

selle lugemine võimatuks. Lisaks peaks hoidma oma prügi ka asutuse väliselt kättesaamatus kohas, et keegi võõras sellele ligi ei pääseks. (Edmead, 2008.)

3.4 Tarkvara uuendamine

Asutused peaksid hoidma oma tarkvara alati uuendatud. Oma rakenduste uuendamisega tagatakse, et töötajatel oleks olemas hetkel kõige turvalisem versioon. Enamus turvaauke, mis avastatakse, parandatakse ja lisatakse uuendusse. Juba vanema Internet Exploreri kasutamine loob palju uusi turvaauke juurde. Kindlasti ei tohiks anda isikutele, kelle identiteedis te kindlad ei ole, infot selle kohta, milliseid veebibrauserit kasutate või mis formaadis tekste avate. (Hadnagy, 2013.) Näiteks võib juhtuda, et sotsiaalmanipulatsiooni rünnaku tegija helistab töötajale ja esitleb end IT-osakonna töötajana, et saada teavet veebibrauseri versiooni kohta. Kui ta saab teada, et kasutatakse uuendamata versioone, siis saab ründaja vastavalt sellele oma rünnakut planeerida.

3.5 Turvaeeskirjad

Turvaeeskirjad on täpsed juhised töötajatele, et võidelda potentsiaalsete turvariskide vastu. Samuti on need olulised sotsiaalmanipulatsiooni rünnakute ennetamiseks ja tuvastamiseks. Turvaeeskirjad ei taga, et alati saab kõiki rünnakuid ennetada. Pigem on eesmärk vähendada riski tasemeni, mis on vastuvõetav. Samuti on oluline, et asutuse kõrgem juhatus näitaks oma tugevat toetust turvaeeskirjade arendamisele. Töötajad peavad nägema, et info turvalisus ja andmete kaitse on ettevõtte toimimise jaoks tähtis. (Mitnick & Simon, 2002.)

Infoturbe eeskirjade kirjutamisel ei tohi kasutada keerulist tehnilist keelt. Peale selle on tähtis kirja panna, miks mingi reegel või protseduur oluline on. Muidu võivad töötajad neid reegleid lihtsalt eirata, sest nad peavad seda ajaraiskamiseks. Töötajatele tuleb teada anda, miks need reeglid on olulised ja millist kahju see võib tuua, kui neid reegleid ei järgita. Lisaks tuleb töötajaid teavitada tagajärgedest, mis neid ootavad, kui nad eeskirju rikuvad. (Mitnick & Simon, 2002.)

Infoturbe eeskirjad ei saa olla muutumatud. Kuna ettevõte ja turvatehnoloogiad võivad muutuda, siis tuleb ka eeskirju regulaarselt üle vaadata ja täiendada. Eeskirjad tuleb panna siseveebi töötajatele kättesaadavasse kohta, et nad sealt vajadusel kiirelt küsimustele vastuseid leiaks. Nõrkade kohtade leidmiseks tuleb perioodiliselt testida eeskirjade järgmist, kasutades sotsiaalmanipulatsiooni meetodeid. (Mitnick & Simon, 2002.)

3.6 Turvaauditid

Asutus võib täiendada küll turvaeeskirju ja töötajaid koolitada, kuid mis siis, kui neid ei võeta tõsiselt või eiratakse. Samuti ei pruugi ettevõte teada, kas ettevõetud toimingud on adekvaatsed või mitte. Sellepärast tulekski teha turvaauditeid. Turvaauditid aitavad tuua välja võimalikke vigu ning tänu sellele saab eeskirju täiendada. Sotsiaalmanipulatsioonile keskenduvate auditite kaudu saab töötajatele näidata, et ka nemad võivad olla sihtmärgiks. (Jones, 2004.)

Enne auditi tegemist on oluline selleks eelnevalt hoolikalt ette valmistada. Kõigepealt tuleks panna paika eesmärk, miks üldse auditit tehakse. Selleks võib olla näiteks uute eeskirjade testimine või ebasobivate toimingute avastamine. Enne testi tegemist tuleb saada nõusolek juhtkonnalt. Peale selle on oluline teavitada töötajaid, et selline turvatest tehakse, kuid te ei pruugi öelda, millal ja keda täpselt testitakse. (Jones, 2004.)

Üks võimalus sotsiaalmanipulatsiooni testi tegemiseks on saata töötajale testmeil. Esmalt kirjutatakse meil, mis sarnaneb tavaliste andmepüügi stsenaariumidega. Seejärel pannakse koostöös IT-osakonnaga üles üks vale veebiaadress, kuhu kasutaja kirjas oleva lingi kaudu suundub. Veebisaidil küsitakse sisse logimiseks vajalikke andmeid. Meil saadetakse töötajatele ja hiljem saab monitoorida, kes nendest lingil klikkisid. (Pyzik, 2015.)

4 UURIMUS

4.1 Metoodika ja valim

Peatükis esitatakse töö eesmärk, uurimisküsimused ja kirjeldatakse uurimismeetodit. Peale selle antakse ülevaade valimist ja selle valiku põhjendustest.

Töö eesmärk on teada saada, kui teadlikud on Tallinna Ülikooli üliõpilased sotsiaalmanipulatsioonist ja selle võtetest. Uurimuse eesmärgist lähtuvalt otsitakse vastust järgmistele uurimisküsimustele.

- Kas Tallinna Ülikooli üliõpilased teavad, mis on sotsiaalmanipulatsioon?
- Kui teadlikud on üliõpilased sotsiaalmanipulatsiooni võtetest?

Uurimuse tegemiseks koostati küsitlus 28 küsimusega (vt lisa 1). Küsimused olid üldised ja enamjaolt valikvastustega. Küsitluse eeliseks on see, et seda on lihtsam jagada suuremale hulgale inimestele ja see võimaldab teada saada üliõpilaste üldist teadmist teema kohta. Küsitluse nõrkade külgedena võib välja tuua, et pole võimalik kontrollida, kas vastajad vastavad ausalt ja kui tõsiselt nad uurimusse suhtuvad. Samuti on raske aru saada, kas vastajad on küsimusi õigesti mõistnud. (Hirsjärvi, Remes & Sajavaara, 2007.)

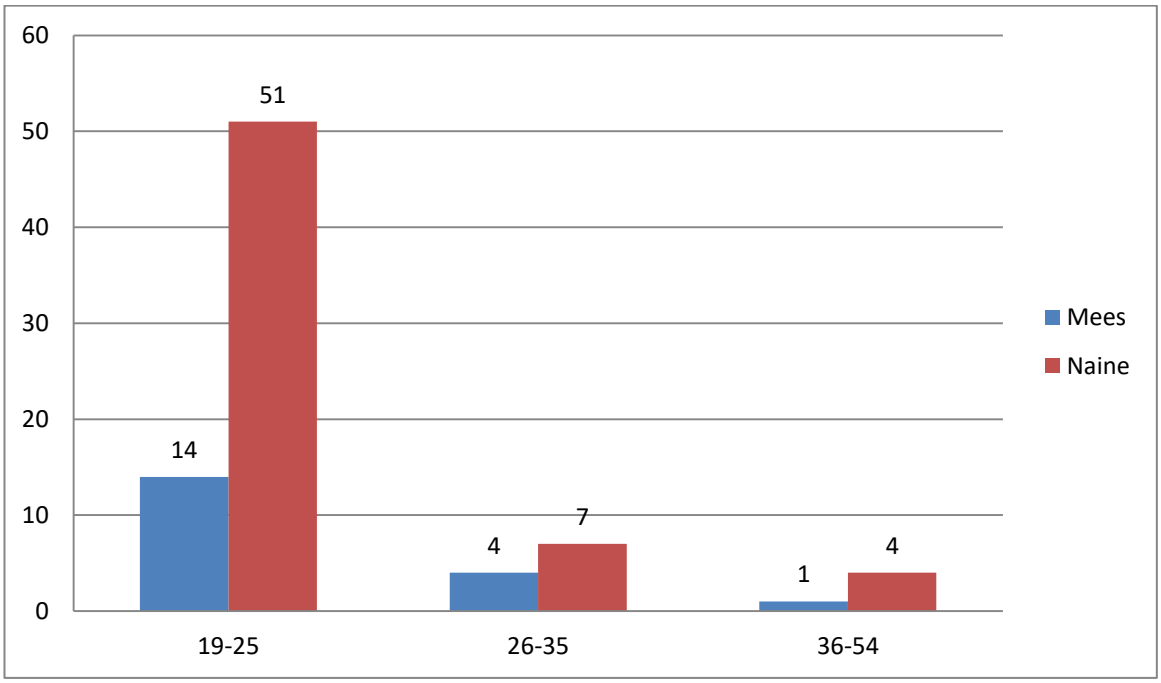
Küsitlus koostati Google Forms keskkonnas. Google Formsi kasuks otsustati, sest see on tasuta, seda on lihtne kasutada, selle jaoks ei pea tegema eraldi kasutajat ja vastuste arv pole piiratud. Peale selle oli hea, et küsitluse vastuste põhjal moodustus automaatselt reaalajas Exceli arvutustabel. Mitmed teised küsitluste keskkonnad nõuavad kasutajaks registreerimist ja nende tasuta variandid ei paku mitmeid olulisi võimalusi.

Küsitlusele saadi vastused kahes Tallinna Ülikooli õppeaines. Kõigepealt jagati küsitlust aines „Arvuti töövahendina“ (kolmes rühmas). Aine valiku kasuks otsustati, sest selles aines osalevad üliõpilased paljudelt erinevatelt erialadelt. Esialgsetest vastustest selgus, et digitehnoloogiate instituudist oli ainult üks vastaja. Seetõttu jagati küsitlust ka ühes informaatika valikaine tunnis. Kokku vastas küsitlusele 81 vastajat kõikidest Tallinna Ülikooli instituutidest.

4.2 Andmete analüüs

Peatükis analüüsitakse küsitluse vastuseid. Kõigepealt kirjeldatakse küsitluses osalejaid vanuse ja soo lõikes. Seejärel tuuakse välja vastused küsimuste kaupa. Selleks, et anda vastustest parem ülevaade, kujutatakse neid joonistena.

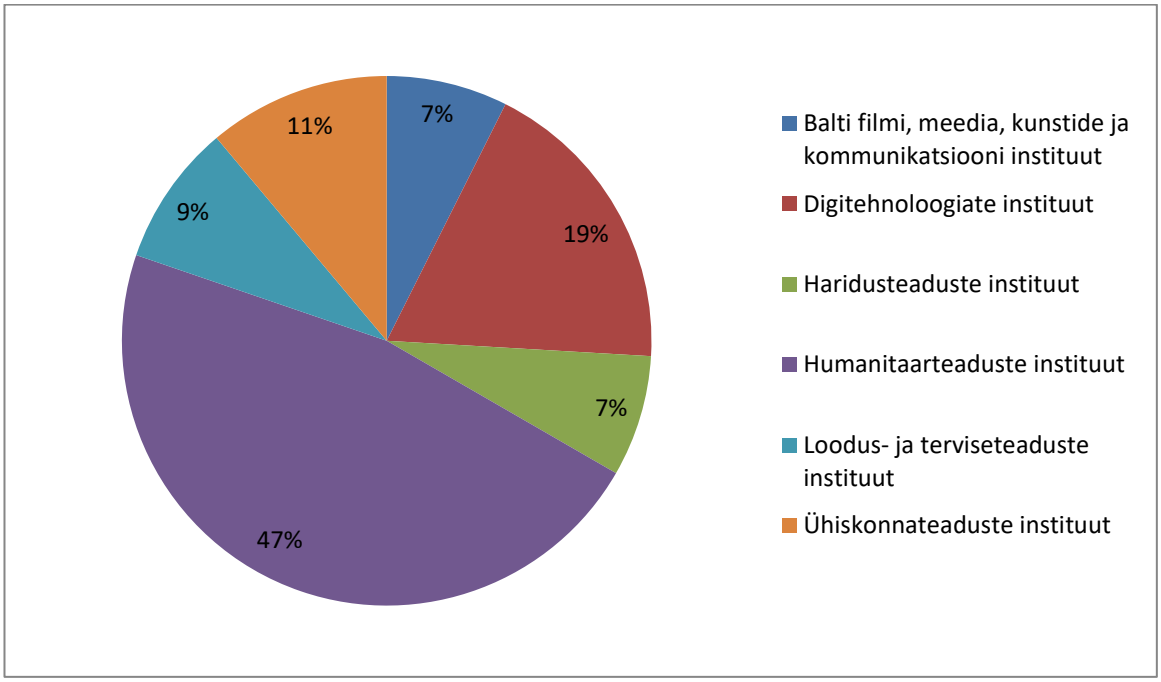
Kokku vastas küsitlusele 81 Tallinna Ülikooli üliõpilast. Neist 62 olid naised ja 19 olid mehed. Kõige rohkem vastanuid oli vanusevahemikus 19–25 aastast. See grupp moodustas 80% vastanutest. Nendest 51 olid naised ja 14 olid mehed. Teise gruppi kuulusid vastajad vanusevahemikus 26–35 aastat. See grupp moodustas 14% vastanutest. Nendest 7 olid naised ja 4 olid mehed. Viimase grupi moodustasid vastajad vanuses 36–54 aastat. See grupp moodustas 6% vastanutest. Nendest 4 olid naised ja 1 oli mees (vt joonis 1).



Joonis 1. Küsitlusele vastanute vanus ja sugu.

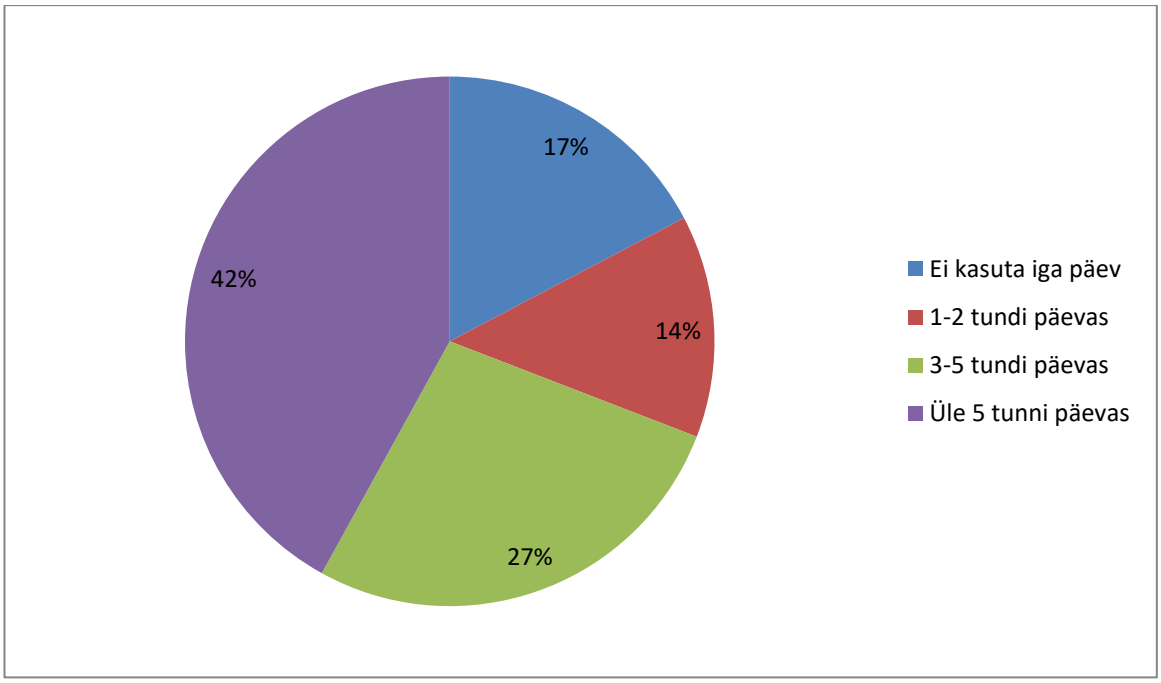
Vastajaid oli kõigist Tallinna Ülikooli instituutidest. Kõige rohkem vastajaid oli humanitaarteaduste instituudist. Sellest instituudist vastas 38 üliõpilast, mis moodustas 47% vastanutest. 15 üliõpilast õppis digitehnoloogiate instituudis (19% vastanutest). Ühiskonnateaduste instituudist oli vastajaid 9, mis moodustas 11% vastanutest. Sellele järgnes loodus- ja terviseteaduste instituut 7 vastajaga (9% vastanutest). Balti filmi,

meedia, kunstide ja kommunikatsiooni ning haridusteaduste instituudist oli mõlemast 6 vastajat. Mõlemad moodustasid 7% vastanutest (vt joonis 2).



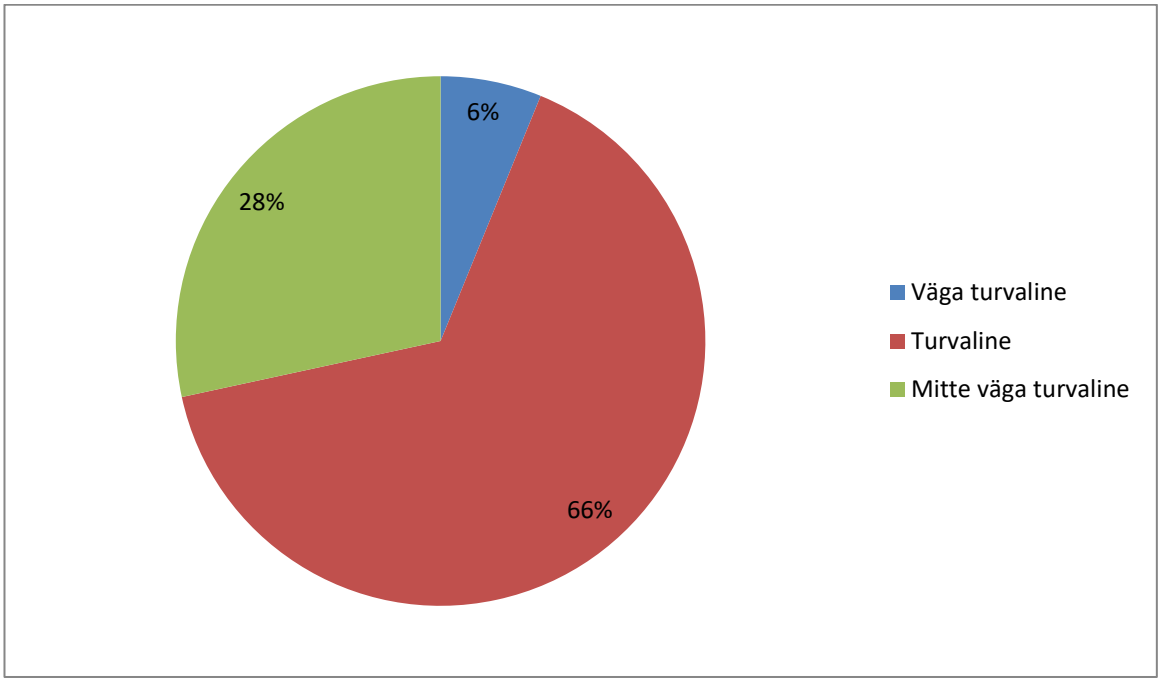
Joonis 2. Vastajad instituutide lõikes.

Küsimusele „Kui tihti kasutate arvutit?“ vastas 42%, et kasutavad arvutit üle 5 tunni päevas. 27% vastanutest kasutavad arvutit 3-5 tundi päevas. 17% vastanutest ei kasuta arvutit iga päev. Vastanutest 14% kasutavad arvutit 1-2 tundi päevas (vt joonis 3). Sellest järeldub, et suur hulk üliõpilastest kasutavad arvutit iga päev. Peale selle saab välja tuua, et üliõpilaste hulk, kes ei kasuta arvutit igapäevaselt on suurem kui nende hulk, kes kasutavad arvutit 1-2 tundi päevas. Kõige rohkem kasutavad arvutit digitehnoloogiate instituudi üliõpilased, kes kasutavad arvutit vähemalt 3 tundi päevas.



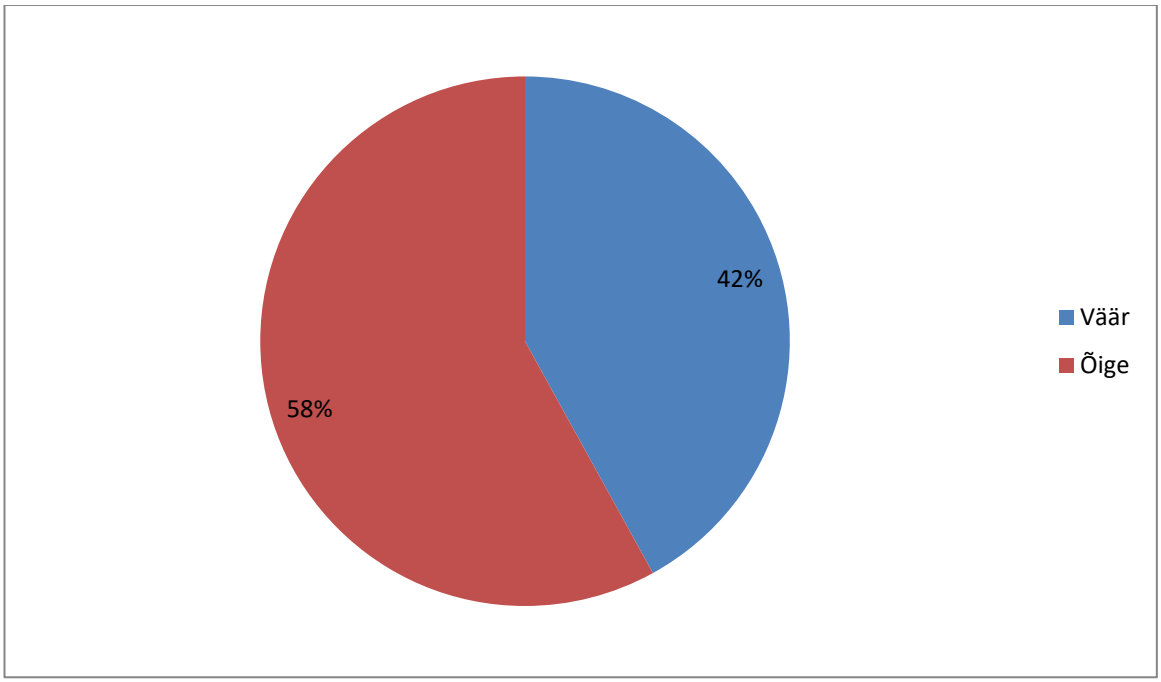
Joonis 3. Kui tihti kasutate arvutit?

Küsimusele „Kui turvaliseks peate oma arvutit?“ vastas 66%, et peavad enda arvutit turvaliseks. 28% vastanutest ei pea enda arvutit väga turvaliseks. Kõigest 6% arvavad, et nende arvuti on väga turvaline (vt joonis 4). Vastustest võib järeldada, et väga vähestel vastanutest on arvuti kõrge turvalisusega.



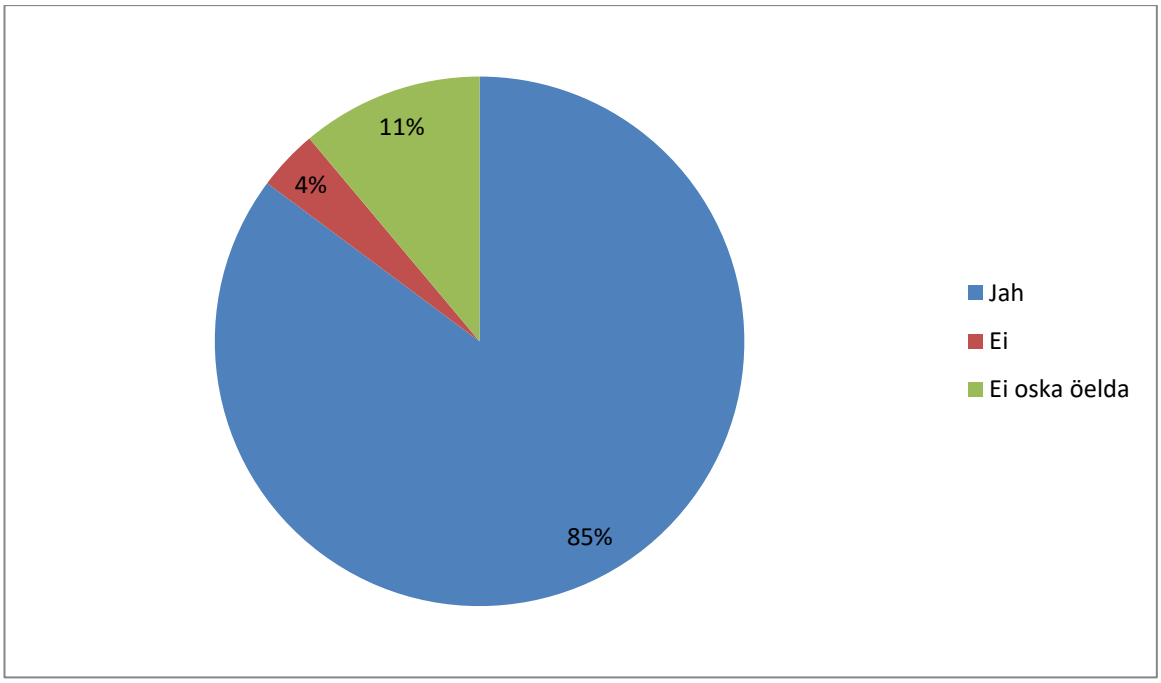
Joonis 4. Kui turvaliseks peate oma arvutit?

Vastanutest 58% arvavad, et nende arvuti pole väärtuslik sihtmärk rünnakutele ja 42% arvavad, et nende arvuti on väärtuslik sihtmärk rünnakutele (vt joonis 5). Sellest järeldub, et üle poole vastanutest arvavad, et nende arvuti ei ole piisavalt tähtis, et keegi võiks seda rünnata.



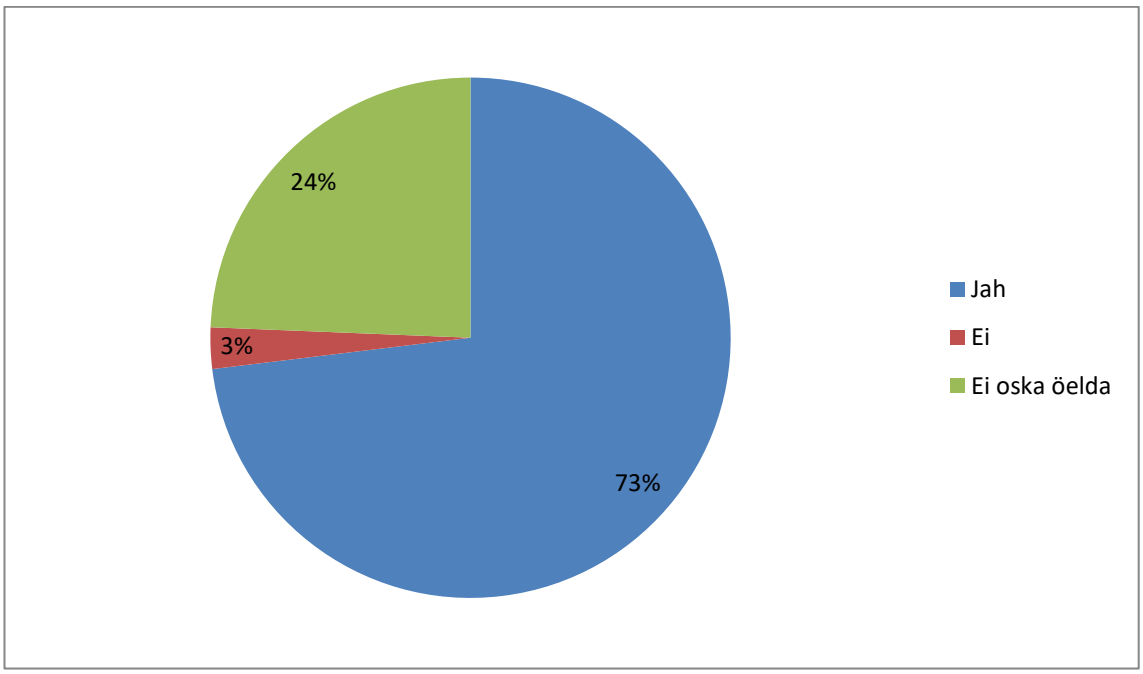
Joonis 5. Minu arvuti pole väärtuslik sihtmärk rünnakutele.

Küsimusele „Kas teie arvutis on viirusetõrjetarkvara?“ vastas 85%, et neil on viirustõrjetarkvara olemas. Vastanutest 11% ei osanud öelda, kas neil on tarkvara viiruste kaitseks või mitte. 4% vastas, et neil puudub viirusetõrjetarkvara (vt joonis 6). Sellest võib järeldada, et enamusel üliõpilastest on mingi viirusetõrjetarkvara olemas, mis aitab nende arvutit võimalike viiruste eest kaitsta.



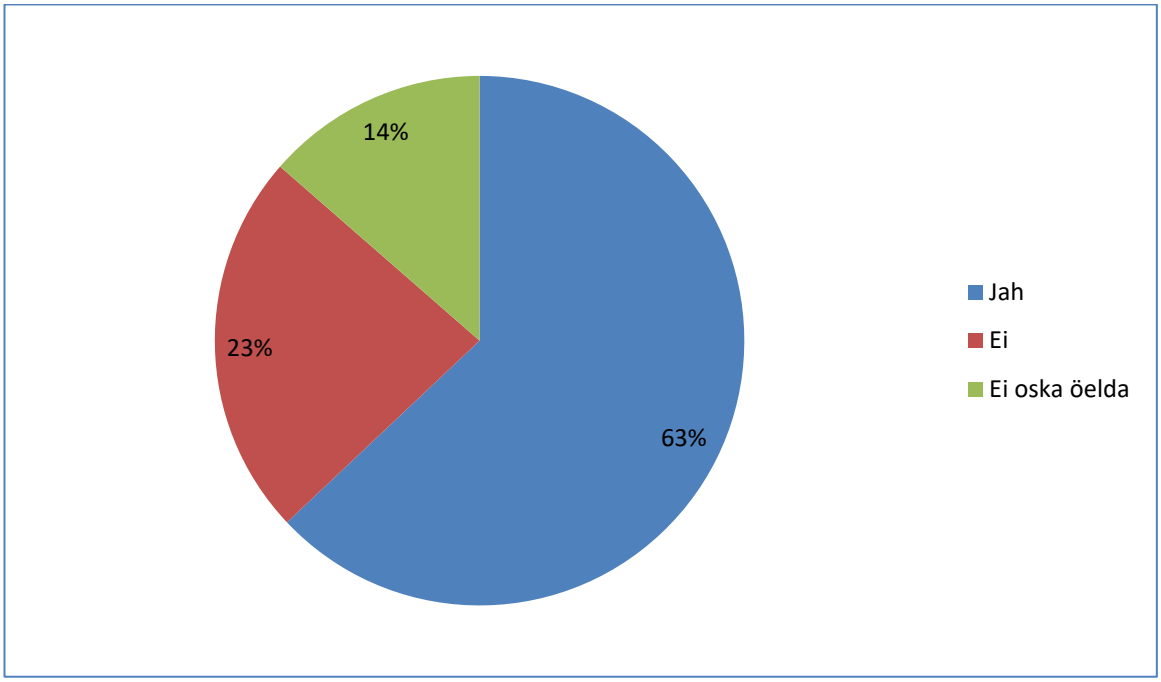
Joonis 6. Kas teie arvutis on viirusetõrjetarkvara?

Peale selle paluti inimestel, kellel tarkvara olemas, täpsustada, kas see on uuendatud ja ajakohane. Üliõpilastest 73%-l on tarkvara uuendatud ja ajakohane. 24% vastanutest ei oska öelda, kas neil on uuendatud ja ajakohane tarkvara. Vastanutest 3%-l ei ole tarkvara uuendatud ega ajakohane (vt joonis 7). Sellest saab järeldada, et suuremal osal üliõpilastest on tarkvara uuendatud ja ajakohane. Analüüsist jäeti välja kolm vastanut, kes olid eelmisele küsimusele vastanud eitavalt.



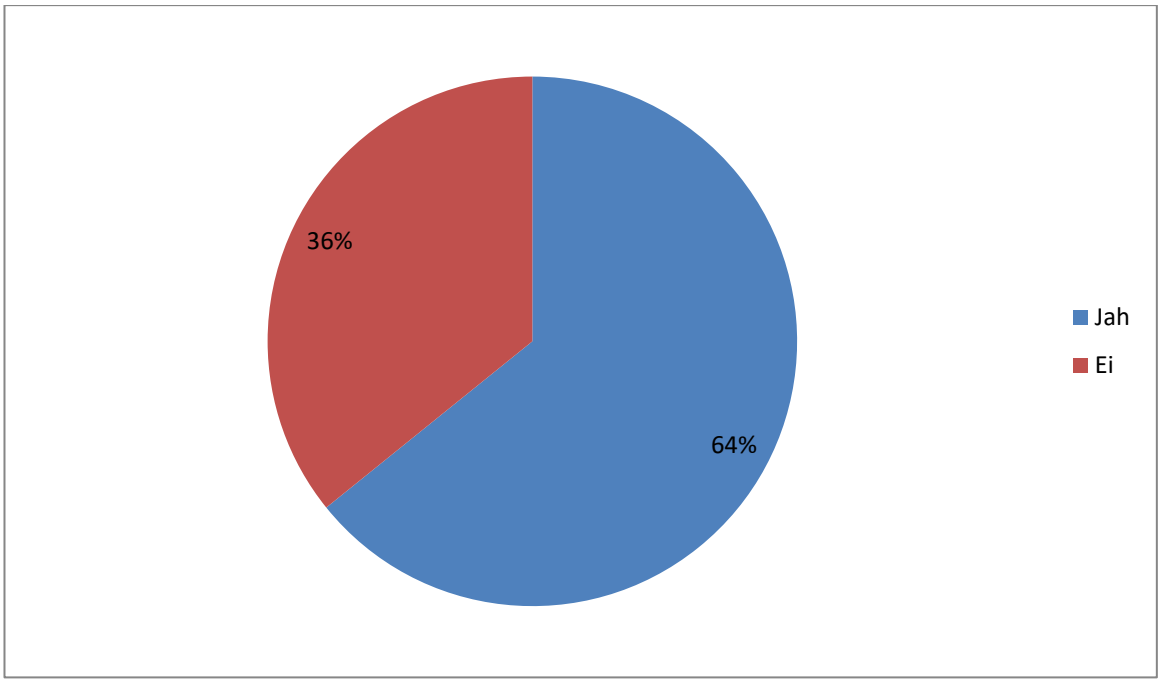
Joonis 7. Kui jah, siis kas see tarkvara on uuendatud ja ajakohane?

Küsimusele „Kas teie arvutis on kunagi olnud viirus või pahavara?“ vastas 63% üliõpilastest, et neil on olnud. Vastanutest 23% ütlesid, et neil ei ole olnud. 14% üliõpilastest ei oska kindlalt öelda, kas neil on olnud või ei ole (vt joonis 8). Sellest võib järeldada, et üle pooltel küsitluses osalenud üliõpilastel on arvuti kunagi nakatunud viiruse või muu pahavaraga. Seega on paljud vastajatest kokku puutunud olukorraga, kus nende arvutit on rünnatud.



Joonis 8. Kas teie arvutis on kunagi olnud viirus või pahavara?

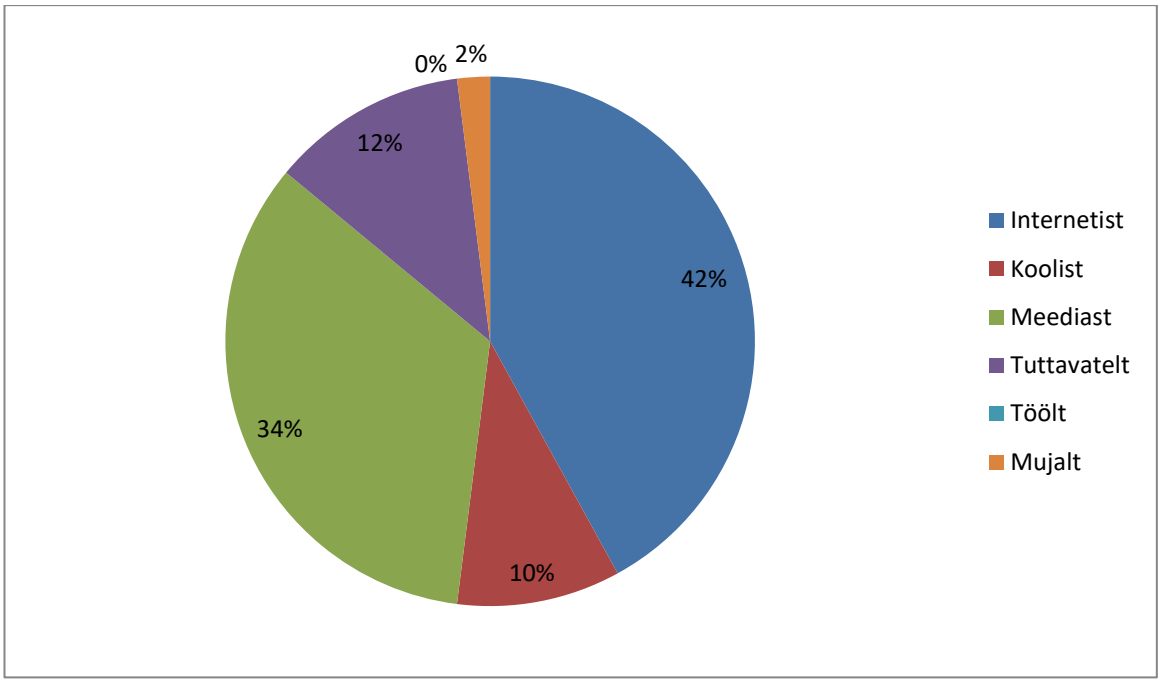
Küsimusele „Kas olete kuulnud sotsiaalmanipulatsioonist (*social engineering*)?“ vastas jaatavalt 64% vastanutest ja eitavalt 36% vastanutest (vt joonis 9). Sellest järeldub, paljud üliõpilased on sotsiaalmanipulatsioonist kuulnud, kuid 29 vastaja jaoks oli see uus mõiste.



Joonis 9. Kas olete kuulnud sotsiaalmanipulatsioonist (*social engineering*)?

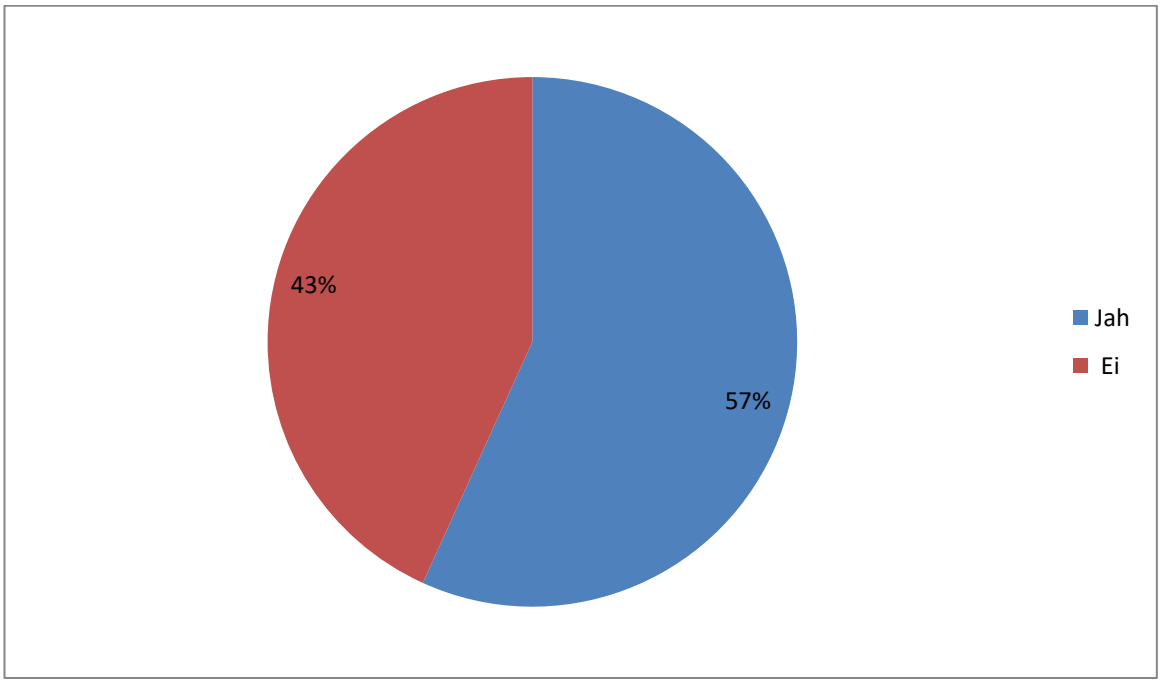
Järgmisena paluti vastajatel täpsustada, millisest allikast nad on teavet saanud. Kõige rohkem on inimesed saanud infot sotsiaalmanipulatsiooni kohta interneti kaudu (42%). Järgmisena on vastajad saanud infot meedia vahendusel (34%). Vastanutest 12% on kuulnud sotsiaalmanipulatsioonist tuttavatelt ja 10% on saanud infot sotsiaalmanipulatsiooni kohta koolist. Mujalt sai infot ainult üks inimene (2%), kes täpsustas, et kuulis sotsiaalmanipulatsioonist filmis. Tööl ei ole mitte ühelegi vastanutest sotsiaalmanipulatsiooni kohta räägitud (vt joonis 10).

Kaks inimest, kes vastasid eelmisele küsimusele „Kas olete kuulnud sotsiaalmanipulatsioonist (*social engineering*)?“ eitavalt, täpsustasid siiski, kust nad selle kohta infot said (meediast ja internetist). Neid vastuseid ei arvestatud selle küsimuse analüüsimisel, sest lähtuti nende esimesest vastusest. Peale selle oli kaks inimest, kes vastasid eelmisele küsimusele „Jah“, kuid ei täpsustanud, millisest allikast nad on infot saanud.



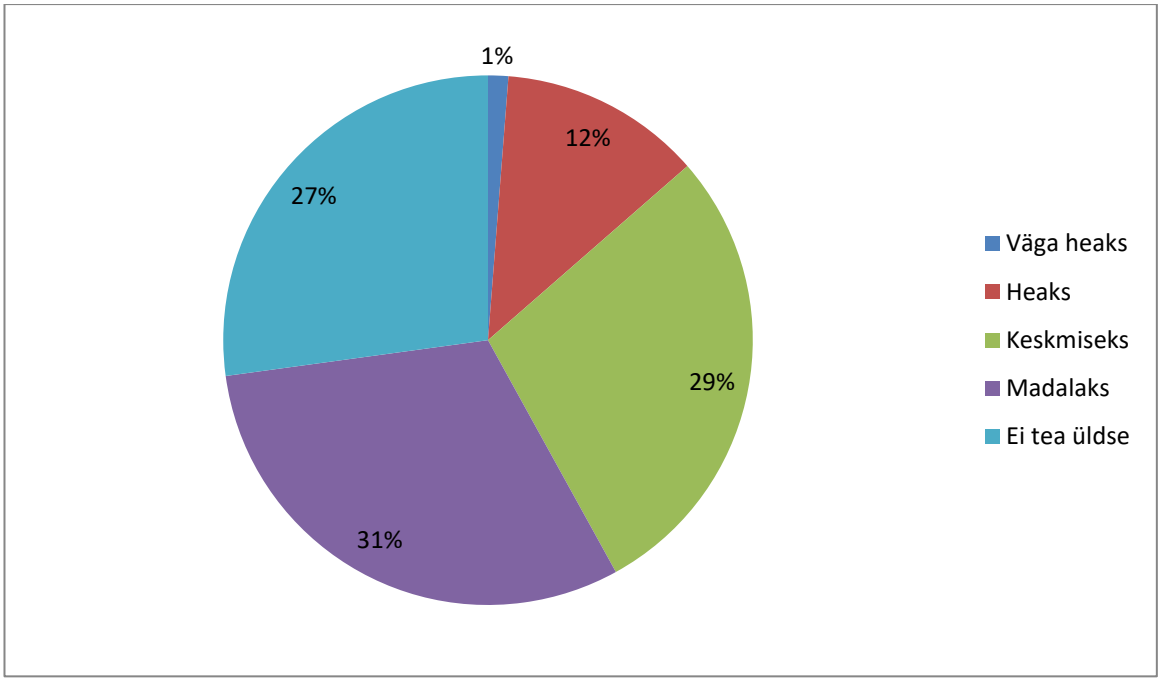
Joonis 10. Kui jah, siis millisest allikast saite infot selle kohta?

Vastanutest 43% väitsid et ei oska enda jaoks sõnastada, mida tähendab sotsiaalmanipulatsioon. 57% vastajatest ütlesid, et oskavad enda jaoks sõnastada, mida tähendab sotsiaalmanipulatsioon (vt joonis 11). Nende tulemuste põhjal võib väita, et alla poole vastanutest ei tea, mida sotsiaalmanipulatsioon endast kujutab.



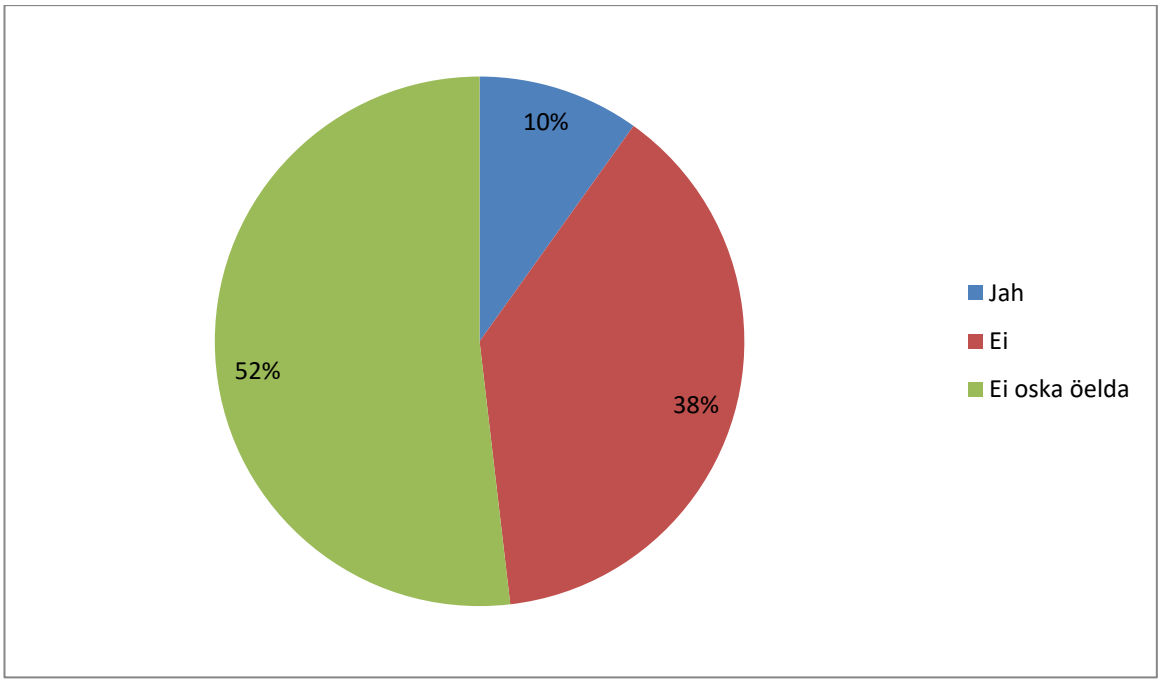
Joonis 11. Kas oskate enda jaoks sõnastada, mida tähendab sotsiaalmanipulatsioon?

Järgmisena küsiti üliõpilastelt, kui heaks nad hindavad oma teadmisi sotsiaalmanipulatsioonist. Kokku üle poole vastanutest peavad oma teadmisi sotsiaalmanipulatsioonist kas madalaks (31%) või ei tea üldse midagi sotsiaalmanipulatsioonist (27%). Vastanutest 12% peavad oma teadmisi heaks. 29% hindavad oma teadmisi keskmiseks ja 1% ehk 1 inimene peab oma teadmisi sotsiaalmanipulatsioonist väga heaks (vt joonis 12). Üliõpilased, kelle teadmised jäävad kas madalaks või ei tea üldse midagi sotsiaalmanipulatsioonist, moodustavad üle poole vastanutest. Sellest võib järeldada, et paljud üliõpilased ei ole kursis sotsiaalmanipulatsiooni ja selle võtetega.



Joonis 12. Kui heaks hindate oma teadmisi sotsiaalmanipulatsioonist?

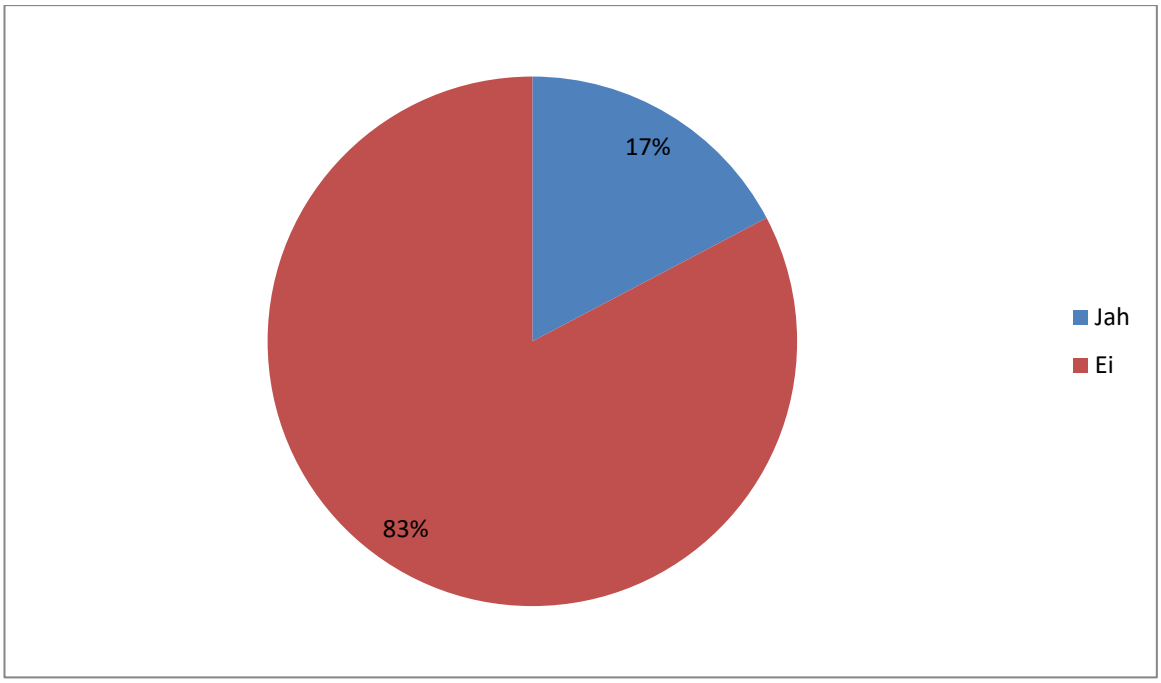
Küsimusele „Kas olete kokku puutunud sotsiaalmanipulatsiooniga?“ vastas 10%, et on kokku puutunud. Vastanutest 38% vastas, et ei ole kokku puutunud. 52% vastajatest ei oska öelda, kas nad on või ei ole kokku puutunud sotsiaalmanipulatsiooniga (vt joonis 13). Paljud inimesed, kes on sotsiaalmanipulatsiooniga mingil moel kokku puutunud, ei saa ise sellest teada. Nende vastuste põhjal saab järeldada, et tegelikult võib neid inimesi, kes on sotsiaalmanipulatsiooniga kokku puutunud, olla rohkem, sest 52% inimestest ei suuda kindlalt öelda, et nad ei ole kokku puutunud sotsiaalmanipulatsiooniga.



Joonis 13. Kas oled kokku puutunud sotsiaalmanipulatsiooniga?

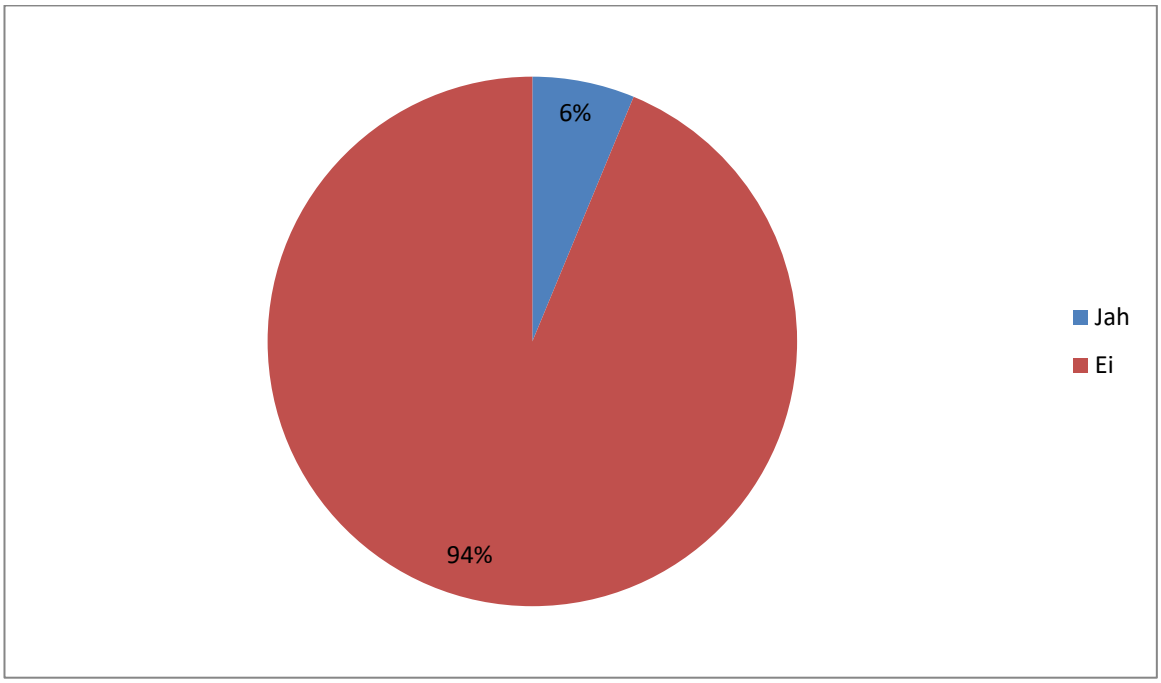
Peale selle paluti nendel, kellel on olnud kokkupuude sotsiaalmanipulatsiooniga, täpsustada, kuidas nad on sellega kokku puutunud. Mitmed üliõpilased tõid välja spämmi ehk rämpsposti. Samuti toodi välja võlts sotsiaalmeediakontod, kes tahavad lisada kasutajat enda sõbraks. Toodi välja ka loosimised sotsiaalmeedias, kus osalemiseks peab jagama oma isikuandmeid. Mainiti ka isikliku meili kasutamist reklaamimisel. Üks üliõpilane tõi välja, et on kokku puutunud võltsmeilide, veebilehtede ja võltskõnedega. Üks vastanu kirjutas täpsustuseks sõna „soorollid“, seetõttu jääb segaseks, mida selle all täpsemalt mõeldi. Võimalik, et vastaja ei ole sotsiaalmanipulatsiooni tähendusega täpselt kursis ja mõistis selle all midagi muud.

Küsimusele „Kas teate kedagi, kes on langenud sotsiaalmanipulatsiooni ohvriks?“ vastas 17%, et teavad kedagi, kes on langenud sotsiaalmanipulatsiooni ohvriks. Vastanutest 83% ei tea kedagi, kellel oleks olnud kokkupuude sotsiaalmanipulatsiooniga (vt joonis 14). Sellest järeldub, et lisaks sellele, et vastanute seas on üliõpilasi, kes on sattunud ise sotsiaalmanipulatsiooni ohvriks, teavad mitmed vastajatest veel inimesi, kes on samuti langenud sotsiaalmanipulatsiooni ohvriks.



Joonis 14. Kas teate kedagi, kes on langenud sotsiaalmanipulatsiooni ohvriks?

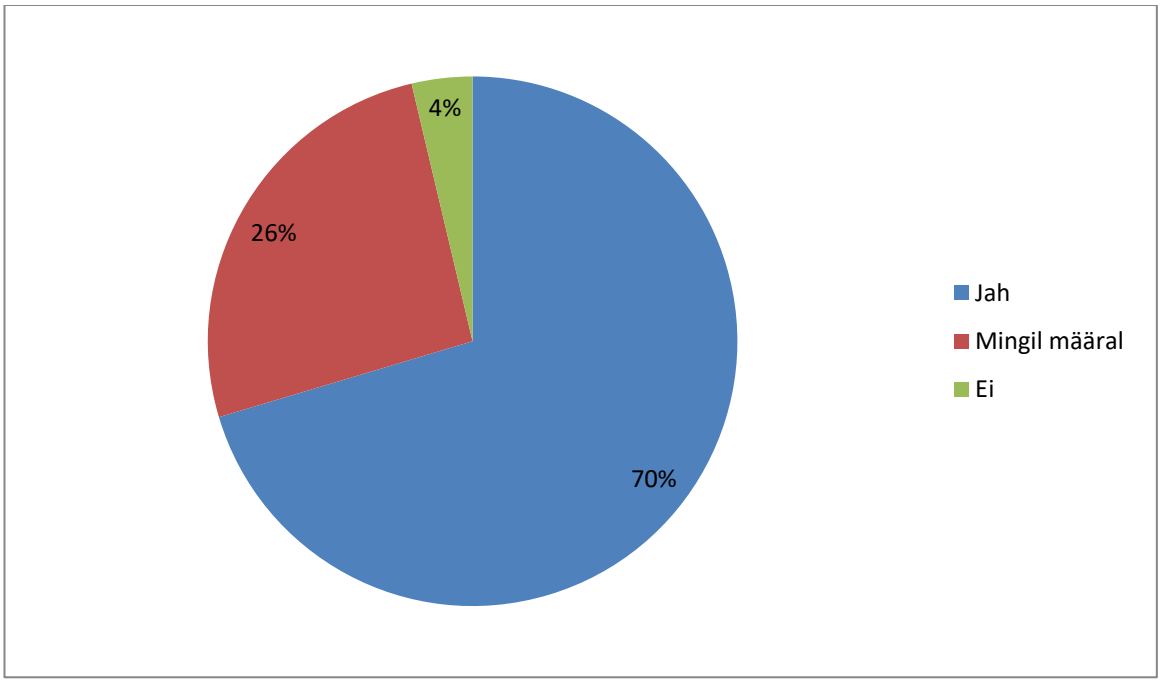
Küsimusele „Kas meili manuse avamine on alati ohutu?“ vastas 6% üliõpilastest, et see on ohutu. 94% vastanutest vastas, et ei ole (vt joonis 15). Selle põhjal saab öelda, et enamus üliõpilasi teavad, et meili manuse avamisel võib olla riskikohti.



Joonis 15. Kas meili manuse avamine on alati ohutu?

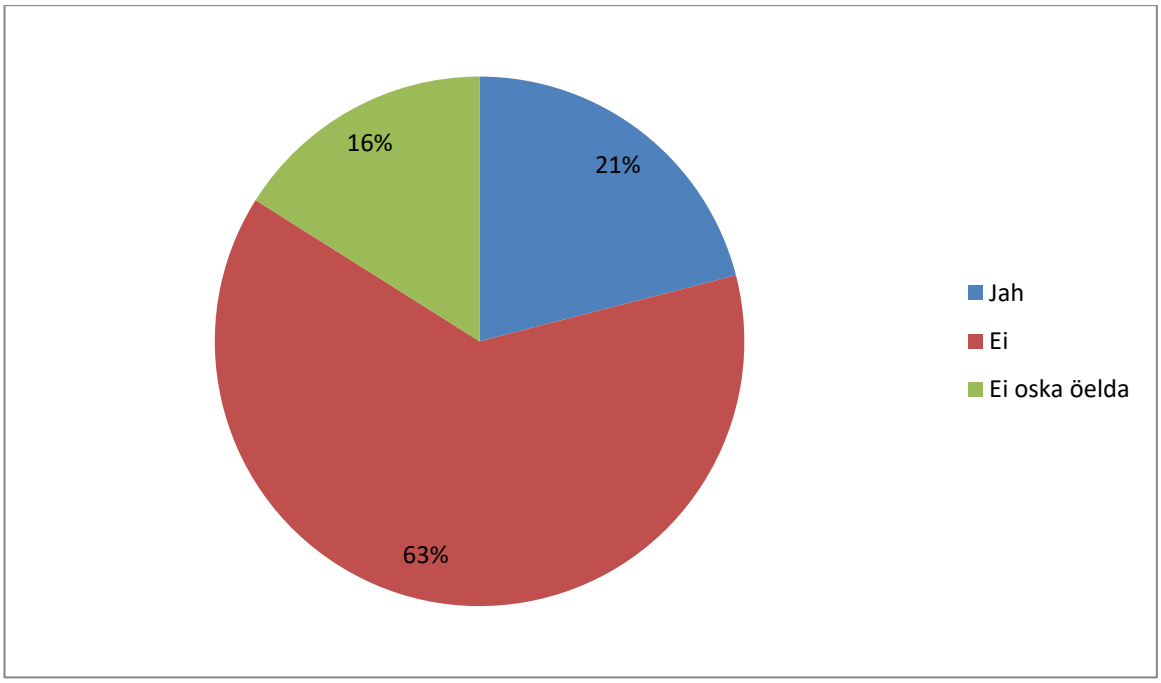
Küsimusele „Kas olete teadlik meilipettustest?“ vastas 70% üliõpilastest, et on küll. 26% vastanutest on meilipettustest teadlik mingil määral. 4% vastanud üliõpilastest aga

ei ole teadlikud meilipettustest (vt joonis 16). Selle põhjal võib järeldada, et suur osa üliõpilastest teavad, kas rohkem või vähem meilipettustest. Kuna 21 inimest vastas, et nad teavad pettustest mingil määral, siis näitab see, et nad pole oma teadmistes väga kindlad.



Joonis 16. Kas olete teadlik meilipettustest?

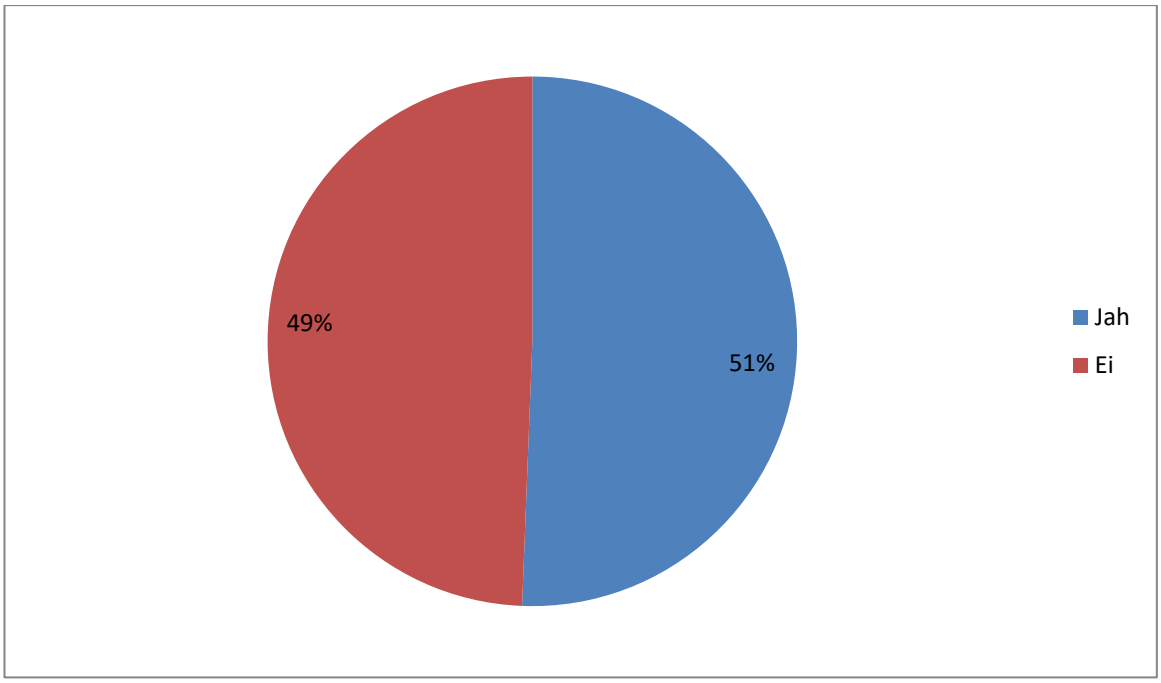
Küsimusele „Kas teie meilikonto või mingi muu konto on kunagi langenud rünnaku või varguse ohvriks?“ vastas 63% üliõpilastest, et ei ole. 16% vastanud üliõpilasest ei oska kindlalt öelda, kas nende meilikonto või mingi muu konto on langenud rünnaku või varguse ohvriks. 21%-l üliõpilastest on meili või mingi muu konto kas varastatud või on seda rünnatud (vt joonis 17). Sellest võib järeldada, et kindlalt ei ole varastatud või rünnatud üle poolte üliõpilaste kontosid. Mitmed üliõpilased on aga sattunud olukorda, kus nende meili- või muud kontod on langenud rünnaku või varguse ohvriks.



Joonis 17. Kas teie meilikonto või mingi muu konto on kunagi langenud rünnaku või varguse ohvriks?

Küsimusele „Kas teate, kuhu pöörduda või mida teha konto varguse korral?“ vastas 51% üliõpilastest, et teavad. 49% vastanud üliõpilastest aga ei tea, kuhu pöörduda või mida teha konto varguse korral (vt joonis 18). Sellest võib järeldada, et peaaegu pooled arvutikasutajatest ei tea, mida teha, kui nende konto peaks langema röövi ohvriks. Vastanute seas oli ka viis üliõpilast, kelle meilikonto või mõni muu konto on juba langenud rünnaku ohvriks ja kes ei tea, kuhu pöörduda või mida teha selles olukorras.

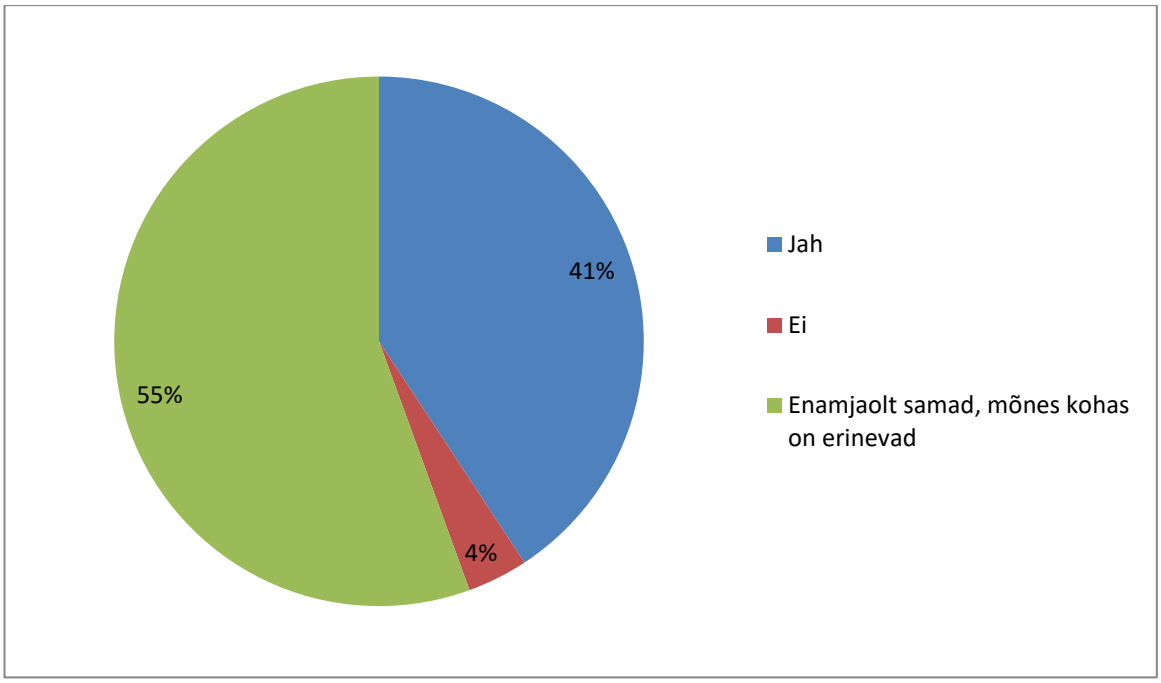
Sellele küsimusele on üks vastustest puudu, sest küsimus ei olnud esimese rühma vastuste ajal märgitud kohustuslikuks. Peale seda märgiti küsimus kohustuslikuks.



Joonis 18. Kas teate, kuhu pöörduda või mida teha konto varguse korral?

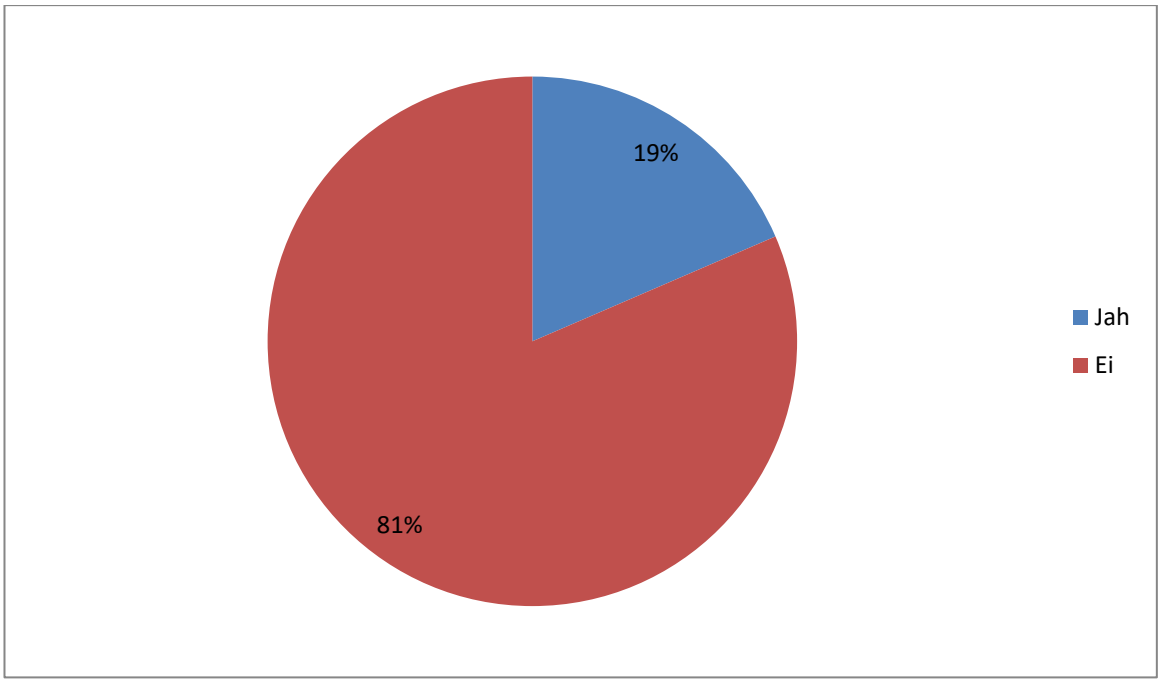
Küsimusele „Kas kasutate erinevaid paroole erinevates kohtades?“ vastas 41%, et kasutavad. 4% vastanud üliõpilastest vastasid, et ei kasuta. Vastanutest 55% väidavad, et kasutavad enamjaolt sama aga mõnes kohas on erinevad (vt joonis 19). Selle põhjal võib väita, et erinevate paroolide kasutamine on üliõpilaste seas küllaltki levinud. Enamus üliõpilasi kasutavad, kas erinevaid paroole või siis mõnedes kohtades erinevaid. Väike osa vastanutest kasutab sama parooli igal pool.

Vastustest selgus, et 8 üliõpilast, kes vastasid eelmisele küsimusele „Kas teie meilikonto või mingi muu konto on kunagi langenud rünnaku või varguse ohvriks?“ jaatavalt, kasutavad enamjaolt sama parooli ja mõnes kohas erinevaid paroole. Samas 9 inimest, kes vastasid samamoodi jaatavalt, kasutavad erinevaid paroole erinevates kohtades.



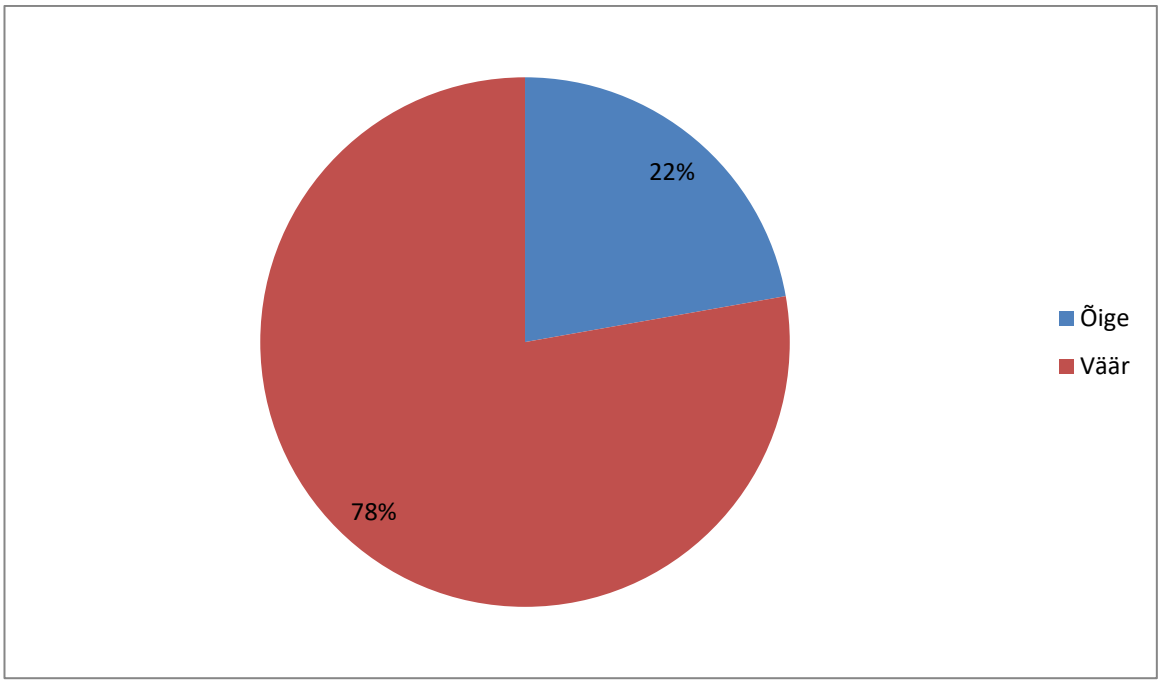
Joonis 19. Kas kasutate erinevaid paroole erinevates kohtades?

Küsimusele „Kas keegi on teilt kunagi küsinud teie parooli“ vastas 81% üliõpilastest, et ei ole. 19%-l vastajatest on olnud olukordi, kus keegi on neilt küsinud nende parooli (vt joonis 20). Sellest saab järeldada, et suuremal osal tudengitest ei ole küsitud nende isiklikku parooli. Peale selle paluti vastajatel täpsustada, mis põhjusel on neilt parooli küsitud. Paljud küsijad on olnud pereliikmed, kes soovivad kasutada arvutit/kontot või teha mingeid muid tegevusi, millest vastanu on olnud teadlik. On olnud ka paar juhtumit, kus on tahetud inimeselt kas kontot varastada või mingit muud kahju teha.



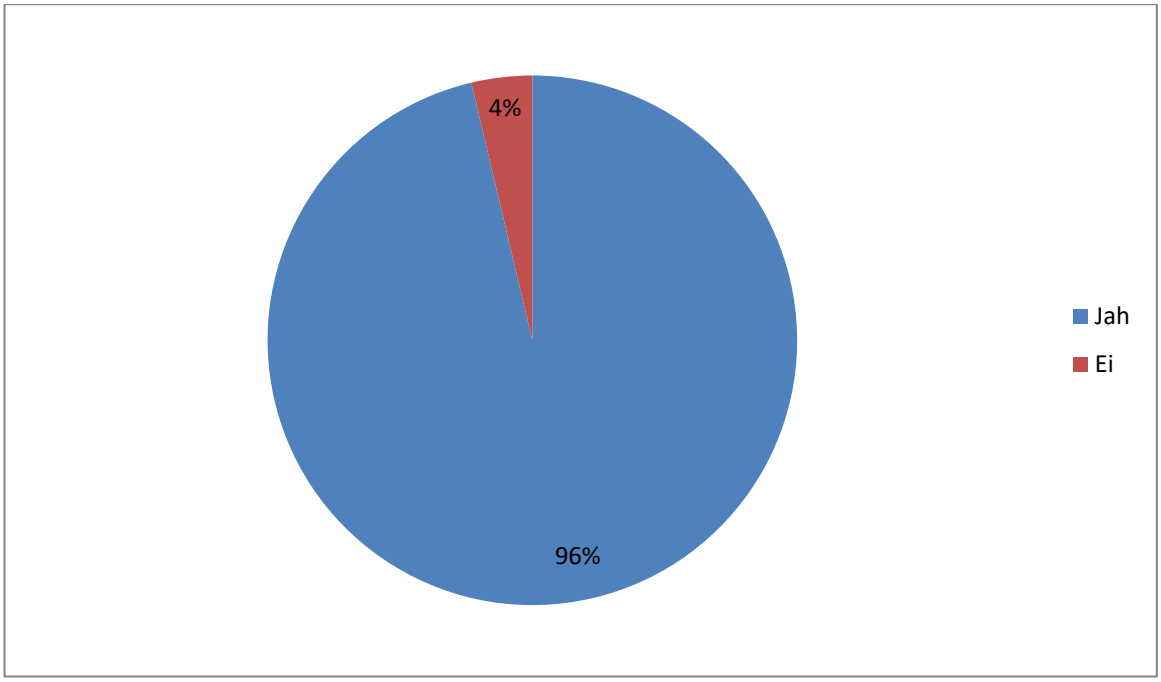
Joonis 20. Kas keegi on teilt kunagi küsinud teie parooli?

Järgmisena esitati üliõpilastele väide „Kui arvutist või USB-mälupulgalt kustutada fail, siis seda ei saa enam taastada“. 78% vastajatest arvasid, et see väide on väär. 22% üliõpilastest arvas, et see väide on õige (vt joonis 21). Sellest võib järeldada, et suur osa üliõpilastest teab, et kõvakettalt või USB-mälupulgalt kustutatud faile on võimalik siiski taastada.



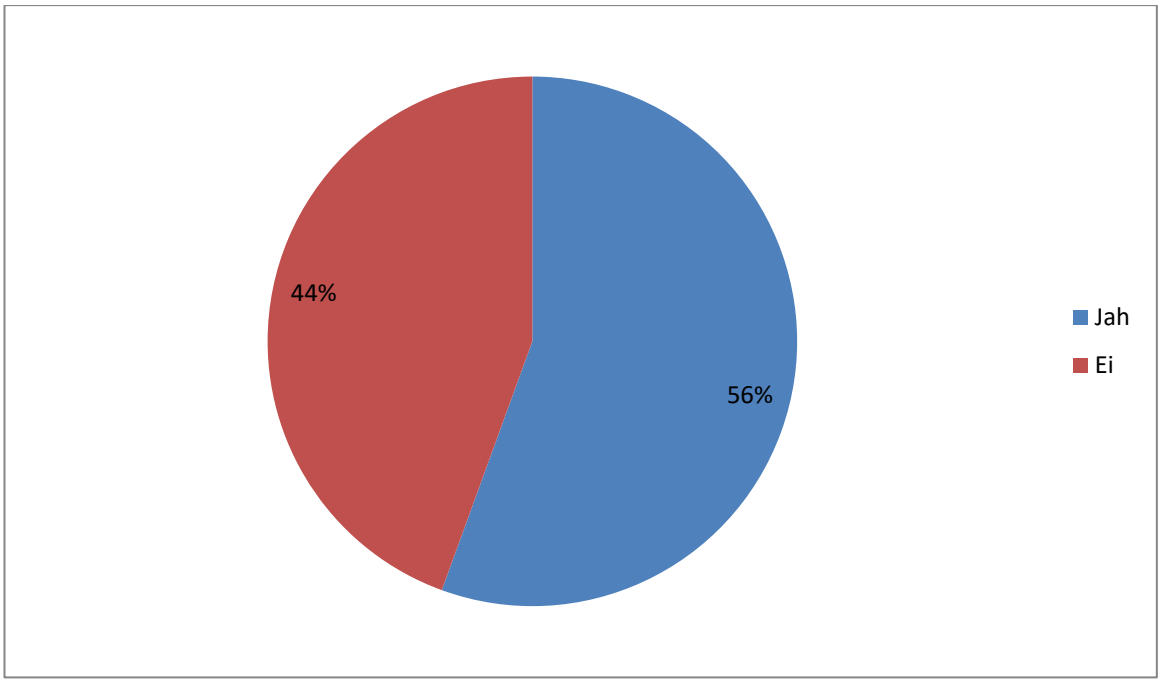
Joonis 21. Kui arvutis või USB-mälupulgalt kustutada fail, siis seda ei saa enam taastada.

Küsimusele „Kas leitud USB-mälupulk võib endast ohtu kujutada?“ vastas 96% üliõpilastest, et jah, võib küll. 4% vastanutest arvab aga, et leitud USB-mälupulk ei kujuta endast ohtu. Sellest võib järeldada, et enamus üliõpilasi teab, et võõras USB-mälupulk võib arvutisse sisestades nakatada arvuti viiruse või mõne muu pahavaraga (vt joonis 22).



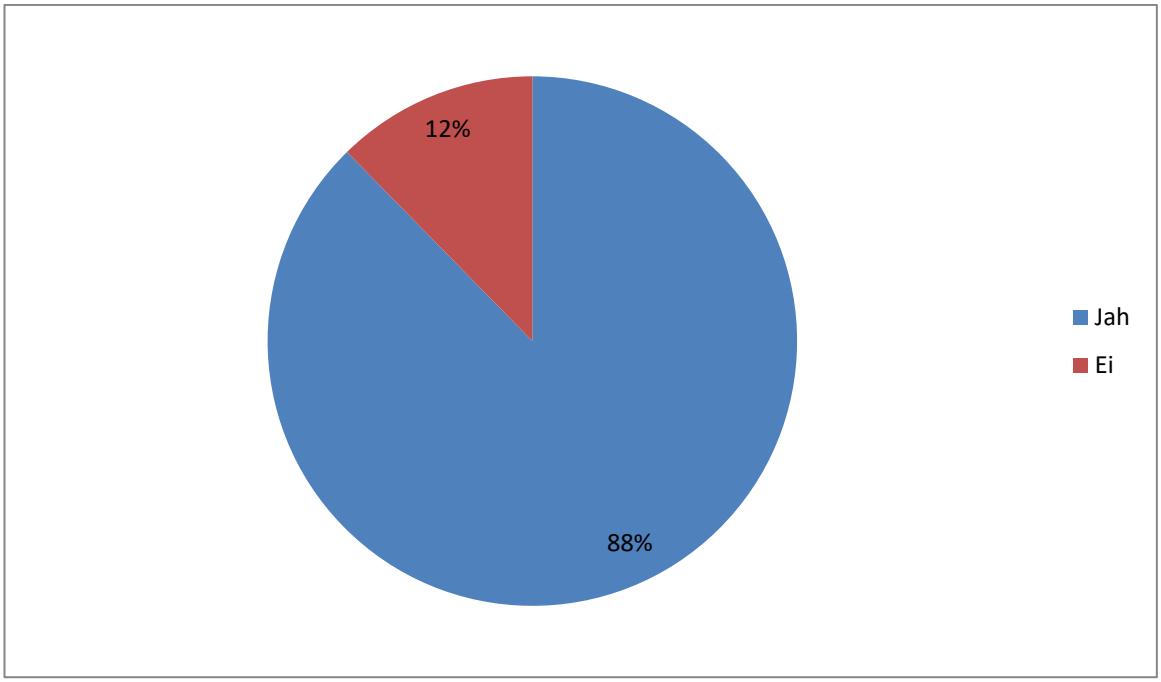
Joonis 22. Kas leitud USB-mälupulk võib endast ohtu kujutada?

Küsimusele „Kas teilt on kunagi telefoni või meili teel küsitud isiklikke andmeid?“ vastas 56% üliõpilastest, et on küll. Vastanutest 44% vastasid, et ei ole (vt joonis 23). Sellest võib järeldada, et üle pooltelt üliõpilastelt on kas telefoni või meili teelt proovitud saada isiklikke andmeid, mis ei ole tegelikult turvaline viis andmeid jagada.



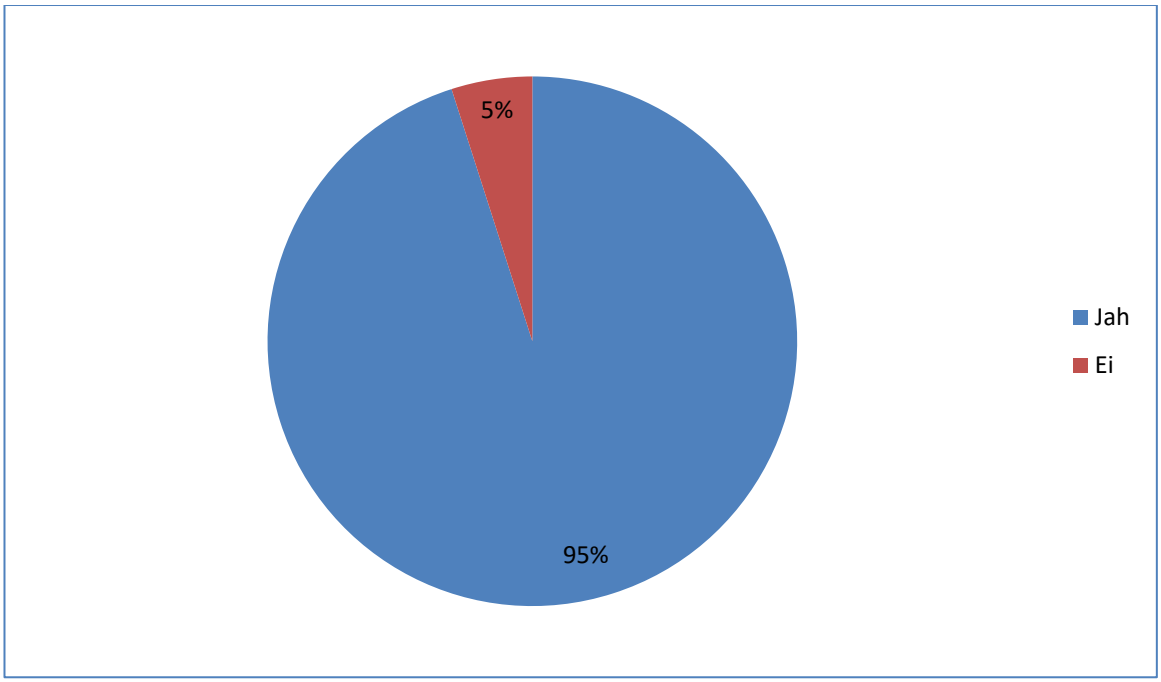
Joonis 23. Kas teilt on kunagi telefoni või meili teel küsitud isiklikke andmeid?

Küsimusele „Kas pangakaardi PIN-koodi sisestamisel avalikus kohas on ohukohti?“ vastas 88% üliõpilastest, et on küll. Vastanutest 12% arvavad, et PIN-koodi sisestamisel avalikus kohas ei ole ohukohti (vt joonis 24). Sellest võib järeldada, et enamus üliõpilasi teab, et pangakaardi PIN-koodi sisestamisel avalikus kohas võib olla riske, sest kunagi ei tea, kes võib üritada sinu PIN-koodi näha.



Joonis 24. Kas pangakaardi PIN-koodi sisestamisel avalikus kohas on ohukohti?

Küsimusele „Kas arvate, et sotsiaalmanipulatsioonist peaks rohkem rääkima?“ vastas 95%, et jah, peaks küll. Vastanutest 5% ei arva, et sotsiaalmanipulatsioonist peaks rohkem rääkima (vt joonis 25). Nendest vastusest võib järeldada, et enamus üliõpilasi sooviks saada rohkem infot sotsiaalmanipulatsiooni kohta.



Joonis 25. Kas arvate, et sotsiaalmanipulatsioonist peaks rohkem rääkima?

4.3 Järeldused

Küsitluse vastustest saab järeldada, et rohkem kui pooled vastajad teavad, mis on sotsiaalmanipulatsioon. Üliõpilaste vastustest selgub, et 64% vastanutest on küll sotsiaalmanipulatsioonist kuulnud, kuid 57% nendest oskab sõnastada, mida see mõiste tähendab. Üliõpilased hindasid oma teadmisi sotsiaalmanipulatsioonist pigem kesiseks. Üliõpilaste hinnang jagunes küllaltki võrdselt keskmise (29%), madala (31%) ja mitte üldse teadmise (27%) vahel. Sellest järeldub, et osa üliõpilastest pole teemaga siiski piisavalt kursis.

Peale selle võib märgata ebakõlasid vastustes. Näiteks kaks inimest vastasid küsimusele „Kas oskate enda jaoks sõnastada, mida tähendab sotsiaalmanipulatsioon?“, et ei oska, aga samas hindasid enda teadmisi sotsiaalmanipulatsioonist heaks. Teise näitena võib tuua selle, et kaks üliõpilast peavad enda arvutit turvaliseks, kuid neil puudub

viirusetõrjetarkvara. Peale selle on 8 üliõpilast, kes ütlevad samuti, et nende arvuti on turvaline või väga turvaline, kuigi nad ei tea, kas nende viirusetõrjetarkvara on uuendatud. Kolmandaks vastasid 4 üliõpilast küsimusele „Kas olete teadlik meilipettustest?“, et nad on teadlikud, kuid samas väitsid ka, et meili manuse avamine on alati ohutu.

Sotsiaalmanipulatsiooni kohta kuuldi erinevatest kanalitest. Põhilised allikad olid internet ja meedia. Keegi ei saanud infot sotsiaalmanipulatsiooni kohta töölt. Selles ei ole tegelikult midagi üllatavat, sest paljud üliõpilased ei pruugi käia tööl. Peale selle ei ole sellest ka palju koolis räägitud, sest sealt sai infot ainult 5 vastajat.

Vastustest selgus, et 58% vastajatest ei arva, et nende arvuti võiks olla väärtuslik sihtmärk rünnakutele. Kui üliõpilased ei pea oma arvutit väärtuslikuks sihtmärgiks, siis ei pruugi nad ka arvuti turvalisusse piisavalt tõsiselt suhtuda. Lisaks võivad nad oma arvutit pidada turvalisemaks, kui see tegelikult on. Näiteks tuli analüüsist välja, et 63% on siiski kokku puutunud viiruste või pahavaraga.

Üldised teadmised peamistest sotsiaalmanipulatsiooni võtetest on üpris head. Vastustest selgus, et üliõpilased võiksid rohkem teada, mida teha, kui neil peaks mõni kasutajakonto langema rünnaku või varguse ohvriks. Pooled vastanutest ei tea, kuidas sellises olukorras käituda või kuhu pöörduda. Ometi on kõigi vastanud üliõpilaste seast 21%-l meilikonto või mõni muu konto langenud rünnaku või varguse ohvriks. Sellest järeldub, et inimeste teadlikkuse sellel teemal on madal ja neid tuleks rohkem teavitada, mida teha konto rünnaku korral. Mida kauem aega möödub konto vargusest, seda rohkem saadakse selle kontoga kahju teha ja seda raskem on seda kontot tagasi saada.

Analüüsi tulemustest selgus, et üle poolte üliõpilaste käest on küsitud telefoni teel isiklikke andmeid. See ei ole hea praktika, sest isiklike andmeid ei tohiks telefoni teel anda. Inimesed ei saa olla päris kindlad, et helistaja on see kellena ta end esitleb.

Üliõpilastest 10% teavad, et on kokku puutunud sotsiaalmanipulatsiooniga. Üle poole vastanutest ei oska öelda, kas nad on sotsiaalmanipulatsiooniga kokku puutunud või mitte. Seega ei saa kindlalt väita, et kokkupuute protsent on ainult 10%, vaid see võib olla suurem. Edukas sotsiaalmanipulatsiooni rünnak ei olegi tavaliselt avastatav alguses. Samuti ei pruukinud vastajad teada, millised tegevused sotsiaalmanipulatsiooni alla liigituvad.

Vastuste analüüsimisel selgus, et mõned küsimused oleks võinud veel lisaks olla, et teha täpsemaid järeldusi. Näiteks oleks võinud küsida veel, kas vastajad käivad tööl. Kuna ükski vastaja ei saanud infot sotsiaalmanipulatsiooni kohta töölt, siis oleks saanud väita, et tööl sellest ei räägita. Teiseks oleks võinud küsida täpsustusi selle kohta, mis põhjusel on inimestelt telefoni teel isiklikke andmeid küsitud ja kas nad ka andsid neid.

Töö andis ülevaate arvutikasutajate üldisest teadlikkusest sotsiaalmanipulatsioonist. See võib olla kasulik teave nii koolile kui ka asustustele, kes tegelevad arvutikasutajate koolitamise ja teavitustööga. Edasi võiks uurida inimeste teadmisi põhjalikumalt (nt intervjuude kaudu) ja teha erinevaid eksperimente.

KOKKUVÕTE

Töö eesmärk oli teada saada, kui teadlikud on Tallinna Ülikooli üliõpilased sotsiaalmanipulatsioonist ja selle võtetest. Teema on aktuaalne, sest küberrünnakud on muutnud järjest sagedamaks. Sellest tulenevalt keskendutakse ka rohkem inimeste turvalisusele veebis ja arvutikasutaja teadlikkuse tõstmisele.

Töö eesmärgist lähtuvalt otsiti vastuseid kahele peamisele uurimisküsimusele.

- Kas Tallinna Ülikooli üliõpilased teavad, mis on sotsiaalmanipulatsioon?
- Kui teadlikud on üliõpilased sotsiaalmanipulatsiooni võtetest?

Töö teoreetilises osas kirjeldati, mis on sotsiaalmanipulatsioon, mille jaoks seda kasutatakse ja mis ajendab sotsiaalmanipulaatoreid. Sotsiaalmanipulatsiooni viise on palju erinevaid, kuid selles töös tutvustati lähemalt kümmet viisi, kuidas inimeste käest vajalikku teavet saada. Kirjeldati nii võtteid, kus tuleb inimestega otse suhelda kui ka kaudselt info hankimise võimalusi. Peale selle toodi välja mõned võtted, kuidas tööandjad saavad ennetada sotsiaalmanipulatsiooni rünnakuid asutustes ja selle kaudu inimeste teadlikkust tõsta.

Selleks, et leida vastused töös püstitatud uurimisküsimustele, viidi läbi küsitlus Tallinna Ülikooli tudengite seas. Valimisse kuulusid ainetes „Arvuti töövahendina“ ja „Veeb ja meedia elemendid“ osalevad üliõpilased. Küsitluses oli 28 küsimust. Kokku vastas küsitlusele 81 üliõpilast kõikidest Tallinna Ülikooli instituutidest.

Tudengite vastuste analüüsist selgus, et rohkem kui pooled vastanutest teadsid, mis on sotsiaalmanipulatsioon. Üldiselt ei hinnanud üliõpilased oma teadmisi sotsiaalmanipulatsioonist heaks. Kõige rohkem infot saadi meediast ja internetist. Sotsiaalmanipulatsiooniga olid kokku puutunud vähesed, kuid üle poole vastajatest ei osanud öelda, kas nad on kokku puutunud või mitte. Peaaegu kõik üliõpilased arvasid, et sotsiaalmanipulatsioonist tuleks rohkem rääkida.

Küsitluses osalenud üliõpilased olid enamasti teadlikud erinevatest sotsiaalmanipulatsiooni viisidest. Näiteks teadsid tudengid meili manustega seotud ohtudest, võõraste USB mälupulkade ohtlikkusest ning seda, et pangakaardi PIN-koodi

sisestamisel avalikus kohas peaks olema teadlik, et keegi võib üritada parooli vaadata. Rohkem tuleb inimeste teadlikkust tõsta selles vallas, mida teha konto rünnakute korral.

SUMMARY

"SOCIAL ENGINEERING AWARENESS AMONG COMPUTER USERS BY THE EXAMPLE OF TALLINN UNIVERSITY STUDENTS"

The aim of this bachelor`s thesis was to find out how aware the students of Tallinn University are on social engineering. This topic is timely because the number of cyber-attacks is growing. Therefore more effort is put into raising the awareness of computer users on social engineering and overall security using the web and computers.

There were two main research questions:

- Do the students of Tallinn University know what social engineering is?
- How aware are the students of Tallinn University on social engineering main methods?

What is social engineering, what is the purpose and what drives social engineers to use them is explained in the theoretical part of this thesis. There are many different methods in social engineering, this thesis describes 10 of them in detail. These methods vary from direct contact with people to more distant approaches. Also methods were presented how to prevent social engineering attacks.

To find answers to the research question a survey was conducted among the students of Tallinn University. Answers were collected from courses „Effective Computer Usage“ and „Web and Media Elements“. There were 28 questions in the survey. Answers form 81 students were collected in the process.

More than half of the students who were part of the survey knew what social engineering is. In general the students did not consider their knowledge on social engineering to be good. Most of the information was gained from media and from the Internet. Few of the students have dealt with social engineering, but more than half of the students were unsure whether they have had contact with social engineering or not. Almost all of the students felt that there should be more discussion about social engineering.

Mostly students knew the main methods of social engineering. For example the dangers concerning email attachments, shoulder-surfing and unknown USB flash drives. More emphasis should be put into raising the awareness of what to do when you email or some other account is stolen.

This thesis showed the overall awareness of social engineering amongst computer users. Further study could contain more detailed study on awareness among people, for example using interviews and some experiments.

KASUTATUD KIRJANDUS

AL-Johani, A. A., & AL-Msloum, A. S. (2013). Social engineering risks in the contemporary reality and methods of fighting these risks. *International Journal of Academic Research Part A, 5*(6), 265-272. doi: 10.7813/2075-4124.2013/5-6/A.33

Allen, M. (2007). *Social Engineering: A Means To Violate A Computer System.* SANS Institute Reading Room. https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529 (19.04.2017).

Ciampa, M. (2011). *Security+ Guide to Network Security Fundamentals, Fourth Edition. 3 Course Technology, Cengage Learning.* http://faculty.olympic.edu/kblackwell/docs/cmptr236/Online%20Book%20Preview/Chapter%202/1111640122_303078.pdf (19.04.2017).

Cyber Security Tips. (2012). *Social Engineering: You are at Risk!* From the Office of Angel Cruz, Chief Information Security Officer, State of Texas, 6 (7). https://www.tamiu.edu/oit/documents/socialengineering1.pdf (19.04.2017).

Edmead, M. T. (2008). *Social engineering attacks: What we can learn from Kevin Mitnick.* http://gauss.ececs.uc.edu/Courses/c6056/pdf/social-engineering-prevent-attacks.pdf (19.04.2017).

Greavu-Şerban, V., & Şerban, O. (2014). Social Engineering a General Approach. *Informatica Economica, 18* (2), 5-14. doi: 10.12948/issn14531305/18.2.2014.01

Hadnagy, C. (2013). *Social Engineering: The Art of Human Hacking.* Indianapolis, Indiana: Wiley Publishing Inc. https://sin.thecthulhu.com/library/security/social_engineering/The_Art_of_Human_Hacking.pdf (12.03.2016).

Hirsjärvi, S., Remes, P., & Sajavaara, P. (2007). *Uuri ja kirjuta.* Tallinn: Medicina

Information Security Office. (kuupäev puudub). *Social Engineering Using a USB Drive.* Garnegie Mellon University. https://www.cmu.edu/iso/aware/be-aware/usb.html (19.04.2017).

Iozzio, C. (2008). *The Cyber Crime Hall of Fame.* http://www.cs.clemson.edu/course/cpsc420/material/Papers/The%20Cyber%20Crime%20Hall%20of%20Fame.pdf (19.04.2017).

Janczewski, L. J., & Fu, L. (2010). Social Engineering-Based Attacks: Model and New Zealand Perspective. *Proceedings of the International Multiconference on Computer Science and Information Technology,* 847–853. https://fedcsis.org/proceedings/2010/pliks/36.pdf (19.04.2017).

Jones, C. (2004). *Social Engineering: Understanding and Auditing.* SANS Institute Reading Room. https://www.sans.org/reading-room/whitepapers/engineering/understanding-auditing-1332 (19.04.2017).

Kikkas, K. (2016, märts). Lihtsalt küsi, ehk turvaründed ilma arvutita. *Nutiajakiri 30+*.

Mitnick, K. D., & Simon, W. L. (2002). *The Art of Deception. Controlling the Human Element of Security.* John Wiley & Sons. http://www.scis.nova.edu/~cannady/ARES/mitnick.pdf (19.04.2017).

Mitnick, K. D., & Simon, W. L. (2011). *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker.* Little, Brown and Company. http://www.pdf-archive.com/2015/10/07/ghost-in-the-wires-kevin-mitnick/ghost-in-the-wires-kevin-mitnick.pdf (19.04.2017).

Pyzik, K. (2015). Shutting the door on social engineering. *Internal Auditor, 72* (5), 20-21. http://web.a.ebscohost.com.ezproxy.tlu.ee/ehost/pdfviewer/pdfviewer?sid=ef9c52f9-4b4f-4120-9017-34c6fb02ef96%40sessionmgr4001&vid=11&hid=4107 (12.03.2016).

LISAD

Lisa 1. Küsitlus

Teadlikkus sotsiaalmanipulatsioonist

* Required

1. Kui tihti kasutate arvutit? *

- ◯ Ei kasuta iga päev
- ◯ 1-2 tundi päevas
- ◯ 3-5 tundi päevas
- ◯ Üle 5 tunni päevas

2. Kui turvaliseks peate oma arvutit? *

- ◯ Väga turvaline
- ◯ Turvaline
- ◯ Mitte väga turvaline

3. Minu arvuti pole väärtuslik sihtmärk rünnakutele *

- ◯ Õige
- ◯ Väär

4. Kas teie arvutis on viirustõrjetarkvara? *

- ◯ Jah
- ◯ Ei
- ◯ Ei oska öelda

5. Kui jah, siis kas see tarkvara on uuendatud ja ajakohane?

- ◯ Jah
- ◯ Ei
- ◯ Ei oska öelda

6. Kas teie arvutis on kunagi olnud viirus või pahavara? *

- ◯ Jah
- ◯ Ei
- ◯ Ei oska öelda

7. Kas olete kuulnud sotsiaalmanipulatsioonist (*social engineering*)? *

- [ ] Jah
- [ ] Ei

8. Kui jah, siis millisest allikast saite infot selle kohta?

- [ ] Internetist
- [ ] Koolist
- [ ] Meediast
- [ ] Tuttavatelt
- [ ] Töölt
- [ ] Muu _____

9. Kas oskate enda jaoks sõnastada, mida tähendab sotsiaalmanipulatsioon? *

- [ ] Jah
- [ ] Ei

10. Kui heaks hindate oma teadmisi sotsiaalmanipulatsioonist? *

- [ ] Väga heaks
- [ ] Heaks
- [ ] Keskmiseks
- [ ] Madalaks
- [ ] Ei tea üldse

11. Kas oled kokku puutunud sotsiaalmanipulatsiooniga? *

- [ ] Jah
- [ ] Ei
- [ ] Ei oska öelda

12. Kui jah, siis mil viisil? (Täpsustage)

_____

_____

_____

13. Kas teate kedagi, kes on langenud sotsiaalmanipulatsiooni ohvriks? *

- [ ] Jah
- [ ] Ei

14. Kas meili manuse avamine on alati ohutu? *

- Jah
- Ei

15. Kas olete teadlik meilipettustest? *

- Jah
- Mingil määral
- Ei

16. Kas teie meilikonto või mingi muu konto on kunagi langenud rünnaku või varguse ohvriks? *

- Jah
- Ei
- Ei oska öelda

17. Kas teate, kuhu pöörduda või mida teha konto varguse korral? *

- Jah
- Ei

18. Kas kasutate erinevaid paroole erinevates kohtades? *

- Jah
- Ei
- Enamjaolt samad, mõnes kohas on erinevad

19. Kas keegi on teilt kunagi küsinud teie parooli? *

- Jah
- Ei

20. Kui jah, siis mis põhjusel?

_____

_____

_____

21. Kui arvutist või USB-mälupulgalt kustutada fail, siis seda ei saa enam taastada *

- Õige
- Väär

22. Kas leitud USB-mälupulk võib kujutada endast ohtu? *

- ◯ Jah
- ◯ Ei

23. Kas teilt on kunagi telefoni või meili teel küsitud isiklikke andmeid? *

- ◯ Jah
- ◯ Ei

24. Kas pangakaardi PIN-koodi sisestamisel avalikus kohas on ohukohti? *

- ◯ Jah
- ◯ Ei

25. Kas arvate, et sotsiaalmanipulatsioonist peaks rohkem rääkima? *

- ◯ Jah
- ◯ Ei

26. Sugu *

- ◯ Mees
- ◯ Naine

27. Vanus *

_____

28. Instituut *

- ◯ Balti filmi, meedia, kunstide ja kommunikatsiooni instituut
- ◯ Digitehnoloogiate instituut
- ◯ Haridusteaduste instituut
- ◯ Humanitaarteaduste instituut
- ◯ Loodus- ja terviseteaduste instituut
- ◯ Ühiskonnateaduste instituut
- ◯ Muu _____