ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Ақпараттық және телекоммуникациялық технологиялар институты

“Киберқауіпсіздік, ақпаратты өңдеу және сақтау” кафедрасы

Сапар Нұрбахыт Ахануұлы

««Әлеуметтік инженерия- қазіргі кездегі кәсіпорындардың АҚ- нің өзекті қатерлерінің бірі»

Дипломдық жұмыс

ТҮСІНІКТЕМЕЛІК ЖАЗБА

Мамандығы: 5В100200 – Ақпараттық қауіпсіздік жүйелері

Алматы 2019

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И.Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Ақпараттық және телекоммуникациялық технологиялар институты

“Киберқауіпсіздік, ақпаратты өңдеу және сақтау” кафедрасы

ҚОРҒАУҒА ЖІБЕРІЛДІ
КАӨжС кафедра меңгерушісі
техн.ғыл.канд. асс.профессор
_____ Н.А.Сейлова
“ 13 ” 05 2019 ж.

Дипломдық жұмыс

ТҮСІНІКТЕМЕЛІК ЖАЗБА

Тақырыбы: “ Әлеуметтік инженерия- қазіргі кездегі кәсіпорындардың АҚ -нің өзекті қатерлерінің бірі ”

Мамандығы: 5В100200 – Ақпараттық қауіпсіздік жүйелері

Орындаған Сапар Н. А.

Пікір беруші
техн.ғыл.канд., МАИН академигі
“Ақпараттық қауіпсіздік
жүйелері” каф. профессоры
_____ С.Т.Тынымбаев
“ _____ ” _____ 2019 ж.

Ғылыми жектекші
техн.ғыл.канд.,
_____ А.Ж.Иманбаев
“ 13 ” 05 2019ж.

Алматы 2019

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Ақпараттық және телекоммуникациялық технологиялар институты

“Киберқауіпсіздік, ақпаратты өңдеу және сақтау” кафедрасы

Мамандығы:5В100200 – Ақпараттық қауіпсіздік жүйелері

БЕКІТЕМІН
КАӨжС кафедра меңгерушісі
техн. ғыл. қанд. асс. профессор
_____ Н.А.Сейлова
“__13__” ___05___ 2019 ж.

Дипломдық жұмыс орындауға
ТАПСЫРМА

Білім алушы *Сапар Нұрбахыт Аханұлы*

Тақырыбы “ Әлеуметтік инженерия қазіргі кездегі кәсіпорындардың АҚ нің өзекті қатерлерінің бірі.”

Университет ректорының 2018 жылғы “16” қазан №1162-б бұйрығымен бекітілген

Аяқталған жұмысты тапсыру мерзімі 2019 жылғы “10”мамыр

Дипломдық жобаның бастап берілістері Ақпаратты қорғау мақсатында әлеуметтік инженериямен танысу және зерттеу

Дипломдық жобада қарастырыатын мәселелер тізімі

а) Ақпарат қауіпсіздігіне әлеуметтік инженериядан келетін қауіп қатер

б) Әлеуметтік инженерия амалдары арқылы ақпараттың сыртқа ағуы

в) Ақпараттың қауіпсіздігін әлеуметтік инженериядан сақтау

Ұсынылатын негізгі әдебиеттер 22 атаудан

1 Кевин Митник, Искусство обмана / Компания АйТи; 2004.

2 Кузнецов М.В. Социальная инженерия и социальные хакеры/ СПб.: БХВ-Петербург,2007.

3 Кевин Митник.. Искусство вторжения: Компания АйТи; 2004..

4 Социальная инженерия //Электронды мәлімет көзі. Элек.журн. EFSOL жүйе интеграциясы 2017. Мәліметке қол жеткізу : https://narfu.ru /agtu /www . agtu.ru
5 Социальная инженерия //Электронды мәлімет көзі. Элек.журн. Ярослав Бабин 2018. Мәліметке қол жеткізу : https://xakep.ru
6 Фишинг-атаки //Электронды мәлімет көзі. Элек.парақ. Владимир Безмалый 2008. Мәліметке қол жеткізу : https://www.osp.ru
7 Как взломать человека //Электронды мәлімет көзі. Элек.парақ. COSSA агентілігі 2017. Мәліметке қол жеткізу : https://www.cossa.ru
8 Технология взлома человека //Электронды мәлімет көзі. Элек.журн. Никита Артемов 2017. Мәліметке қол жеткізу : https://medium.com
9 Социальная инженерия как метод взлома человека //Электронды мәлімет көзі. Элек.журн. Habr 2018. Мәліметке қол жеткізу : https://habr.com
10 Social Engineering //Электронды мәлімет көзі. Элек.журн. Imperva 2018. Мәліметке қол жеткізу : https://www.imperva.com
11 What is Social Engineering //Электронды мәлімет көзі. Элек.парақ. Robert Ikovly 2018. Мәліметке қол жеткізу : https://www.webroot.com
12 Social Engineering //Электронды мәлімет көзі. Элек.журн. Кевин Бивер2017. Мәліметке қол жеткізу : https://searchsecurity. Techtarget . com
13 More than one in 10 employees fall for social engineering attacks //Электронды мәлімет көзі. Элек.журн. Warrick Ashford 2018. Мәліметке қол жеткізу : https://www.computerweekly.com
14 Кристофер Хаднаджи Unmasking the Social Engineer: The Human Element of Security// By SPACED,2014.
15 Шарон Конхеди Social Engineering in IT Security: Tools, Tactics, and Techniques// ABC-CLIO,2014.
16 Social Engineering //Электронды мәлімет көзі. Элек.журн. Джефф Биккерс 2019. Мәліметке қол жеткізу : https://www.social-engineer.com/
17 Phishing //Электронды мәлімет көзі. Элек.парақ. Phishing inc 2019. Мәліметке қол жеткізу : http://www.phishing.org
18 Phishing //Электронды мәлімет көзі. Элек.журн. Imperva 2018. Мәліметке қол жеткізу : https://www.imperva.com
19 Уил Аллсопп Unauthorised Access: Physical Penetration Testing For IT Security Teams // A John Wiley and Sons, Ltd., Publication 2009.
20 Кристофер Хаднаджи, Мишел Финчер Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails //Gannett Company 2015.
21 Социальная инженерия: Quid Pro Quo атаки //Электронды мәлімет көзі. Элек.журн. М Салман Надим 2015. Мәліметке қол жеткізу : https://blog.mailfence.com
22 5 Types of Social Engineering Attacks //Электронды мәлімет көзі. Элек.журн. KATIE THORNTON 2018. Мәліметке қол жеткізу : https://www.datto.com

Дипломдық жұмысты дайындау

КЕСТЕСІ

Бөлімдер атауы, қарастырылатын мәселелер тізімі	Ғылыми жетекші мен кеңесшілерге көрсету мерзімдері	Ескерту
Ақпарат қауіпсіздігіне әлеуметтік инженериядан келетін қауіп қатер	15.02.19 - 20.02.19	
Әлеуметтік инженерия амалдары арқылы ақпараттың сыртқа ағуы	27.02.19 - 19.03.19	
Ақпараттың қауіпсіздігін әлеуметтік инженериядан сақтау	20.03.19 - 30.04.19	

Дипломдық жұмыс бөлімдерінің кеңесшілері мен норма бақылаушыларының аяқталған жұмысқа қойған **қолтаңбалары**

Бөлімдер атауы	**Кеңесшілер, аты, әкесінің аты, тегі (ғылыми дәрежесі, атағы)**	**Қол қойылған күні**	**Қолы**
Норма бақылау	А.А.Зиро, тех. ғыл. магистрі, лектор	13.05.19	

Ғылыми жетекші _____ А.Ж.Иманбаев

Тапсырманы орындауға алған білім алушы _____ Сапар Н.А.

Күні “13” 05 2019 ж.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ және ҒЫЛЫМ МИНИСТРЛІГІ
СӘТБАЕВ университеті

ҒЫЛЫМИ ЖЕТЕКШІНІҢ ПІКІРІ

Дипломдық жобаға
(жұмыс түрлерінің атауы)
Сапар Нұрбахыт Ахануұлы
(студенттің аты жөні)
5В100200-Ақпараттық қауіпсіздік жүйелері
(мамандық атауы мен шифрі)

Тақырыбы: «Әлеуметтік инженерия – қазіргі кездегі кәіпорындардың АҚ–нің өзекті қатерлерінің бірі»

Дипломдық жұмыста, студентке қойылған мақсат: әлеуметтік инженерияға практикалық жұмыстар жасай отырып өзектілігін дәлелдеу және қарсы тұру жолдарын ұйымдастыру. Жоғарыда келтірілген мақсатқа қол жеткізу үшін, келесі міндеттер қойылды :

1. Әлеуметтік инженерия амалдарын зерттеп, әр амалға практикалық жұмыс жасады
2. Эксперттердің кеңестерін талдай отырып, қарсы тұру амалдарын құрды

Автор әлеуметтік инженерияның өзектілігін айқындап көрсете білді. Әлеуметтік инженерияның амалдарын орындау барысында фишинг, претекстинг, кви про кво, трояндық вирусқа және жолдағы алма әдістеріне ерекше көңіл бөлді. Претекстинг амалына практикалық жұмыс жасау нәтижесінде адамның мінез құлқы когнитивтік бұрмалануға ұшырайтынын дәлелдеді. Кви про кво әдісін зерттеп, әлеуметтік инженериядан зардап шегуші тек жеке адам емес кіші, орта және ірі компаниялар бола алатынын көрсете білді. Практикалық жұмыстардың нәтижесін зерттей келе және эксперттердің кеңестеріне көңіл бөліп әлеуметтік инженерияға қарсы амалдар құрды. Әлеуметтік инженерия амалдарына практикалық жұмыс жасау арқылы, объект және субъектілерін анықтады. Дипломдық жұмысты толығымен уақытында орындай алды.

Сапар Нұрбахыт "Әлеуметтік инженерия қазіргі кездегі кәсіпорындардың ақпараттық қауіпсіздігінің өзекті қатерлерінің бірі" тақырыбындағы дипломдық жобасы ҚазҰТЗУ университетінің дипломдық жобаға қойылатын талаптарына сәйкес келеді, ал оның авторы ақпараттық қауіпсіздік жүйесін дайындау бағыты бойынша бакалавр біліктілігін алуға лайық.

Ғылыми жетекші

Техникалық ғылымдарының магистрі.
(қызметі, ғыл. дәрежесі, атағы)
_____ Иманбаев А. Ж.

«13» 05 2019 ж

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
СӘТБАЕВ УНИВЕРСИТЕТІ

РЕЦЕНЗИЯ

_____ Дипломдық жұмыс _____
(жұмыс түрінің атауы)

_____Сапар Нұрбахыт Ахануұлы_____
(білім алушының Т.А.Ә.)

5В100200 – «Ақпараттық қауіпсіздік жүйелері» мамандығы

_____
(мамандық атауы мен шифрі)

Тақырыбы: Әлеуметтік инженерия қазіргі кездегі кәсіпорындардың АҚ нің өзекті қатерлерінің бірі

Орындалды:
а) графикалық бөлім _____ парақ
б) түсініктеме _____ бет

ЖҰМЫСҚА ЕСКЕРТУ

Қазіргі кезде ақпарат ең құнды және ең құпиялы құбылыстардың бірі болып табылады. Қазір ақпаратты әр түрлі мақсатта қолдану мүмкін. Мысалы, ақпаратты сатуға, өз игілігіне қолдануға немесе ақпарат арқылы біреуді бопсалауға, мәжбүрлеуге және тағы да басқа әрекеттерде қолданылуы мүмкін. Үстіде келтірілген себептерге сай қазіргі таңда ақпараттың құны өсуде. Ақпараттың құны өскен сайын, оны қолына түсіргісі келетін адамадар саны геометриялық прогрессияда өсуде. Ақпарат әр- түрлі күйде болады (параққа жазылған сөздер, дауыс, электронды түрде және т.б.). Ақпараттың келбеті, түрі көп болғанына байланысты, зиянкестер ақпаратты заңсыз жолмен қолына жеткізу үшін сәйкесінше әр түрлі амалдарды қолдануда. Бұл амалдардың ішінде әлеуметтік инженерияда бар.

Дипломдық жұмысымның тақырыбын әлеуметтік инженерия деп таңдағанымның себебі, қазіргі кезде әлеуметтік инженерия өте өзекті мәселелердің бірі болып табылады. Бұған дәлел осы жылдағы әлеуметтік инженерияға тап болған зардап шегушілер саны 65% өсті. . Әлеуметтік инженерия ұғымы шыққан кезден бастап бұл ұғым бір мезетке де өз өзектілігін жоғалтқан жоқ, керісінше өзінің өзектілігін ұлғайтуда. Қазіргі кезде ақпараттың ұрлануының 70% әлеуметтік инженерия арқылы жүзеге асырылады. . Компания әлемдегі ақшаға сатып алуға мүмкін ең үздік қорғану жүйелерін сатып алатын болса да, жұмыскерлерін жұмыс орнынан шыққан сайын құпия ақпаратты тығып кетуге үйретсе де, әлемдегі ең үздік күзет

орындарынан күзетшілерді жалдайтын болса да бұл компания толығымен осал болып келеді. Бұл осалдылықты алдын алу немесе қарсы тұру үшін дипломдық жұмысымда әлеуметтік инженерияны толығымен зерттеп, практикалық жұмыстар жасадым.

Графикалық материалдары: Әлеуметтік инженерияға практикалық мысалдар. Сұлба ретінде келтірілген статистикалар.

Студент Сапар Н.А. дипломдық жұмысты орындау кезінде өзінің жұмысқа деген ынтасын, оқу кезінде алған теориялық білімін практикада дұрыс қолдана білетіндігін айқын түрде көрсеткен.

ЖҰМЫСТЫҢ БАҒАСЫ

Дипломдық жұмысты «___98___» бағалаймын және Сапар Н.А. 5В100200 мамандығы бойынша әскери іс және қауіпсіздік бакалавры деген біліктілікке лайық деп санаймын.

Пікір беруші
техн.ғыл.канд., МАИН академигі
“Ақпараттық қауіпсіздік жүйелері”
кафедрасы профессоры _____С.Т.Тынымбаев

«08» 05 20 19 ж.

Отчет подобия

SATBAYEV UNIVERSITY

Университет:	Satbayev University
Название:	Әлеуметтік инженерия - қазіргі кездегі кәсіпорындардың АҚ - нің өзекті қатерлерінің бірі
Автор:	Сапар Нұрбахыт
Координатор:	Азамат Иманбаев
Дата отчета:	2019-05-04 16:42:13
Коэффициент подобия № 1: ?	**0,1%**
Коэффициент подобия № 2: ?	**0,0%**
Длина фразы для коэффициента подобия № 2: ?	**25**
Количество слов:	7 563
Число знаков:	61 127
Адреса пропущенные при проверке:	
Количество завершенных проверок: ?	37

К вашему сведению, некоторые слова в этом документе содержат буквы из других алфавитов. Возможно - это попытка скрыть позаимствованный текст. Документ был проверен путем замещения этих букв латинским эквивалентом. Пожалуйста, уделите особое внимание этим частям отчета. Они выделены соответственно.
Количество выделенных слов 4

Самые длинные фрагменты, определеные, как подобные

№	Название, имя автора или адрес гиперссылки *(Название базы данных)*	Автор	Количество одинаковых слов	Удалить отмеченное

1	URL_ http://kk.convdocs.org/docs/index-28795.html	5

Документы, в которых найдено подобные фрагменты: из RefBooks

i

Не обнаружено каких-либо заимствований

Документы,содержащие подобные фрагменты: Из домашней базы данных

Не обнаружено каких-либо заимствований

Документы,содержащие подобные фрагменты: Из внешних баз данных

Не обнаружено каких-либо заимствований

Документы,содержащие подобные фрагменты: Из интернета

Документы, выделенные жирным шрифтом, содержат фрагменты потенциального плагиата, то есть превышающие лимит в длине коэффициента подобия № 2

№	Источник гиперссылки	Количество одинаковых слов (количество фрагментов)	Удалить отмеченное
1	URL_ http://kk.convdocs.org/docs/index-28795.html	5 (1)	

Детали отчета подобия

Фрагменты, найденные в документах базы данных отмечены красным цветом.
Фрагменты, найденные в интернете отмечены в зеленый .
Фрагменты, найденные в базе данных Юридических актов отмечены синим фоном .

Протокол анализа Отчета подобия

заведующего кафедрой / начальника структурного подразделения

Заведующий кафедрой / начальник структурного подразделения заявляет, что ознакомился(-ась) с Полным отчетом подобия, который был сгенерирован Системой выявления и предотвращения плагиата в отношении работы:

Автор: Сапар Нұрбахыт

Название: Әлеуметтік инженерия - қазіргі кездегі кәсіпорындардың АҚ - нің өзекті қатерлерінің бірі

Координатор: Азамат Иманбаев

Коэффициент подобия 1:0,1

Коэффициент подобия 2:0

Тревога:4

После анализа отчета подобия заведующий кафедрой / начальник структурного подразделения констатирует следующее:

☑ обнаруженные в работе заимствования являются добросовестными и не обладают признаками плагиата. В связи с чем, работа признается самостоятельной и допускается к защите;
☐ обнаруженные в работе заимствования не обладают признаками плагиата, но их чрезмерное количество вызывает сомнения в отношении ценности работы по существу и отсутствием самостоятельности ее автора. В связи с чем, работа должна быть вновь отредактирована с целью ограничения заимствований;
☐ обнаруженные в работе заимствования являются недобросовестными и обладают признаками плагиата, или в ней содержатся преднамеренные искажения текста, указывающие на попытки сокрытия недобросовестных заимствований. В связи с чем, работа не допускается к защите.

Обоснование:

.....
.....
.....
.....
.....

.....

Дата 13.05.19г

.....

Подпись заведующего кафедрой

начальника структурного подразделения

Окончательное решение в отношении допуска к защите, включая обоснование:

.....
.....
.....
.....
.....

....

Дата 13.05.19г. *Подпись заведующего кафедрой /*

начальника структурного подразделения

Протокол анализа Отчета подобия Научным руководителем

Заявляю, что я ознакомился(-ась) с Полным отчетом подобия, который был сгенерирован Системой выявления и предотвращения плагиата в отношении работы:

Автор: Сапар Нұрбахыт

Название: Әлеуметтік инженерия - қазіргі кездегі кәсіпорындардың АҚ - нің өзекті қатерлерінің бірі

Координатор:Азамат Иманбаев

Коэффициент подобия 1:0,1

Коэффициент подобия 2:0

Тревога:4

После анализа Отчета подобия констатирую следующее:

☑ обнаруженные в работе заимствования являются добросовестными и не обладают признаками плагиата. В связи с чем, признаю работу самостоятельной и допускаю ее к защите;

☐ обнаруженные в работе заимствования не обладают признаками плагиата, но их чрезмерное количество вызывает сомнения в отношении ценности работы по существу и отсутствием самостоятельности ее автора. В связи с чем, работа должна быть вновь отредактирована с целью ограничения заимствований;

☐ обнаруженные в работе заимствования являются недобросовестными и обладают признаками плагиата, или в ней содержатся преднамеренные искажения текста, указывающие на попытки сокрытия недобросовестных заимствований. В связи с чем, не допускаю работу к защите.

Обоснование:

.....
.....
.....
.....
.....
.....

13.05.2019 г.

Дата

Подпись Научного руководителя

АҢДАТПА

Ұсынылған дипломдық жұмыстың мақсаты - әлеуметтік инженерияны толығымен зерттеу және әлеуметтік инженерияның амалдарын практикалық және теориялық жағынан қарастыру. Зерттеу барысында жиналған ақпаратты қолдана отырып, әлеуметтік инженерияға қарсы тұру немесе алдын алу шараларын ұйымдастыру.

Дипломдық жұмысты жазу барысында қойылған міндеттер:

1. Әлеуметтік инженерияны толығымен зерттеу.
2. Әлеуметтік инженерия амалдарына практикалық жұмыс жасау арқылы, объект және субъектілерін анықтау.
3. Әр жасалған практикалық жұмысты зерттеу. Объект және субъектілерін зерртеу арқылы, алдын алу немесе қарсы тұру жолдарын қарастыру.
4. Эксперттердің оқиғаларын және кеңестерін қарастыру.

Дипломдық жұмыстың ерекшелігі- әлеуметтік инженерияның амалдарын практикалық түрде зерттеп және сәйкесінше қарсы тұру жолдарын қарастыру.

Практикалық жұмыстардың объектілері: жеке тұлға және компания.

Жоғарыда берілген мақсаттар мен міндеттер жұмыс барысында орындалады.

АННОТАЦИЯ

Целью дипломной работы является изучение социальной инженерии, а также изучение теоретических и практических аспектов социальной инженерии. Организация профилактики социальной инженерии по итогам исследования и изучения собранных материалов.

Задачи, поставленные во время написания дипломной работы:

1. Полностью изучить социальную инженерию;
2. Определить объекты и субъекты, путем практической работы над аспектами социальной инженерии;
3. Исследование каждой выполненной работы. Определить способы предотвращения и профилактики, путем изучения объектов и субъектов;
4. Изучить советы и истории экспертов.

Особенностью дипломной работы является практическая работа над методами социальной инженерии и способов их предотвращения. Объектами практических работ являются человек и частная компания. Вышеуказанные цели и задачи будут выполнены в данной работе.

ANOTATION

The aim of the thesis is the study of social engineering, as well as the study of theoretical and practical aspects of social engineering. Organization of prevention of social engineering based on the results of research and study of the collected materials.

The tasks posed during the writing of the thesis:

1. Fully study social engineering;
2. Identify objects and subjects through practical work on aspects of social engineering;
3. Study of each work performed. Identify ways to prevent and resist, by examining objects and subjects;

Learn tips and stories from experts.

The peculiarity of the thesis is the practical work on social engineering methods and ways to prevent them. The objects of practical work are a person and a private company. The above goals and objectives will be fulfilled in this work.

МАЗМҰНЫ

КІРІСПЕ

Бұл дипломдық жұмыс ақпараттың қауіпсіздігі және әлеуметтік инженерия жайында көптеген ақпарат береді.

Бірінші, мен ақпараттық қауіпсіздіктің ең осал тұсын көрсетіп, неге жұмыскер немесе компания әлеумеметтік инженерлердің шабуылдарына ұшарауы мүмкін екендігін түсіндірдім.

Екіншіден, әлеуметтік инженерлер адамдардың сенімдерімен, пайдалы болғысы келетін сезімдерімен, кішіпейілдігімен қолданып, өзіне керек ақпаратты қалай алатынын түсіндіремін. Әлеуметтік инженерлердің әр-түрлі бас киімдермен және әр- түрлі келбеттерде болуы үшін кез келген оқиғаны ойлап табатындығын көрсеттім. Егер сіз әлеуметтік инженерлермен ешқашан кездеспедім деп ойласаныз, сіздің қателесуіңіз әбден мүмкін.

Үшіншіден, әлеуметтік инженерлер өзінің қалаған мақсаттарына жеткенін көрсетемін. Әлеуметтік инженерлер әр-түрлі амалдарды қолдана отырып, компанияларға кіріп өзін қызықтыратын ақпаратты ұрлағанын көрсетемін.

Төртіншіден, әлеуметтік инженериядан қорғану әдістерін зерттедім. Әйгілі әлеуметтік инженерлердің және эксперттердің кеңестерін оқып, өзім бірнеше әдіс ойлап таптым.

1 Әлеуметтік инженерияның өзектілігі

Қазіргі кезде ақпарат ең құнды және ең құпиялы құбылыстардың бірі болып табылады. Қазіргі кезде ақпараттар әр түрлі мақсатта қолданылуы мүмкін. Мысалы, ақпаратты сатуға, өз игілігіне қолдануға немесе ақпарат арқылы біреуді бопсалауға, мәжбүрлеуге және тағы да басқа әрекеттерде қолданылуы мүмкін. Үстіде келтірілген себептерге сай қазіргі таңда ақпараттың құны өсуде. Ақпараттың құны өскен сайын, оны қолына түсіргісі келетін адамдар саны геометриялық прогрессияда өсуде. Ақпарат әр- түрлі күйде бола алады (параққа жазылған сөздер, дауыс, электронды түрде және т.б.). Ақпараттың келбеті, түрі көп болғанына байланысты, зиянкестер ақпаратты заңсыз жолмен қолына жеткізу үшін сәйкесінше әр түрлі амалдарды қолдануда. Бұл амалдардың ішінде әлеуметтік инженерияда бар.

Дипломдық жұмысымның тақырыбын әлеуметтік инженерия деп таңдағанымның себебі, қазіргі кезде әлеуметтік инженерия өте өзекті мәселелердің бірі болып табылады. Бұған дәлел осы жылдағы әлеуметтік инженерияға тап болған зардап шегушілер саны 65%-ға өсті. Зардап шегушілер қатарында жеке тұлғалар, кіші орта және ірі кәсіпорындар бар. Әлеуметтік инженерия ұғымы шыққан кезден бастап бұл ұғым бір мезетке де өз өзектілігін жоғалтқан жоқ, керісінше өзінің өзектілігін ұлғайтуда. Бұл өзектілік ұлғайған сайын, әлеуметтік инженерияны заңсыз жолмен қолданғысы келетін адамдар саны ұлғайып жатыр. Қазіргі кезде ақпараттың ұрлануының 70% әлеуметтік инженерия арқылы жүзеге асырылады. Бұл пайыздарға дәлел соңғы кезде үлкен және орта корпорацияларға жасалған 20 шабулдардың 12-сі әлеуметтік инженерия арқылы жасалған, бұл 70 пайыздан астамы. Ал корпорацияларды ғана емес, барлық шабуылдарға келетін болсақ бұл пайыз 90-ға жетеді. Әлеуметтік инженерияның қарқынды даму себебі, барлық жүйеде ең осал ол техника емес, адам болып табылады. Қазіргі таңда әлеуметтік инженерия арқылы жасаған шабуылдардан зардап шегушілер шамамен 25 000- 100 000 доллар арасында қаражат жоғалтады. Компания әлемдегі ақшаға сатып алуға мүмкін ең үздік қорғану жүйелерін сатып алатын болса да, жұмыскерлерін жұмыс орнынан шыққан сайын құпия ақпаратты тығып кетуге үйретсе де, әлемдегі ең үздік күзет орындарынан күзетшілерді жалдайтын болса да, бұл компания толығымен осал болып келеді. Жұмыскерлер, эксперттер кеңес берген ақпараттық қауіпсіздіктің ең үздік ережелерімен жүрсе де, жаңа шыққан ережелерді мүлк етпей орындаса да толығымен осал болып есептеледі.

Бұған дәлел Ресей мемлекетінде 2018 жылы банктерден, орта және үлкен компаниялардан шамамен 750 млн. руб. әлеуметтік инженерия арқылы ұрланған. Банктердің қауіпсіздігі үздік технологиялармен қорғалады. Бірақ бұл технологиялар адамның мінез құлық, әдеттерінін осалдылығына қарсы тұра алмайды. Сондықтан тек технологияларды күшейтумен тоқтап қалмай, жұмыскерлердің шеберліктерін күшейту керек.

Әлеуметтік инженериядан қорғану үшін, ол алдымен не екенін толығымен зерттеу керек.

2 Әлеуметтік инженерияның пайда болу уақыты, тарихы

Әлеуметтік инженерия тұралы ең алғашқы рет 70-ші жылдардың басында естіле бастады. Ол кездері жүйелер өте қарапайым болған. Қарапайым болғанның өзінде жүйелер тек ірі корпорацияларда болған. Осы кезде компьютерлік технологияларда әлеуметтік инженерия түсінігі пайда болды. Бұл уақытта әлі компьютерлік жүйелер болмаған, бірақ телефонды жүйелер болған. Ал жүйе бар жерде хакерлер бар, нақтылай айтсам фрикерлер.

Фрикерлердің ең алғашқы қызуғушылықтарының бірі, операторларға қоңырау шалып олардың құзыреттіліктері туралы сөйлесіп, мазақ қылу. Операторлар, әсіресе жаңа жұмыскерлерден олар таныс емес ақпарат сұраған кезде, жұмыскерлер ақтала бастайтын. Біраз уақыт өткеннен кейін, зиянкестер бұл әдісті тек қызықшылық мақсатында емес, ақпаратты заңсыз жолмен алу мақсатында қолданған. 70-ші жылдардың соңына таман әлеуметтік инженерияның бұл әдісі дамығаны соншалықты, тәжірибелі фрикер жұмыскерден өзіне керек ақпараттың бәрін алып қолданатын.

Келесі қадамда компьютерлік жүйелер пайда болды. Бұрында фрикерлер операторлардың құлақтарына отырып, сол арқылы керек ақпаратты алатын. Ал қазіргі кезде бір құпия сөз арқылы бүкіл ақпаратты алу мүмкіндігі пайда болды.

Фрикинге мысал келтірсем, 1970 жылдары Кевин Митниктің алдын ала дайындықтан өткен фрикингтік қоңырауларын атап көрсетуге болады. Кевин Митник телефонын келесі жағында отырған жұмыскерге сенімді болып көрінуі үшін, компанияның әр түрлі бөлімшелерін зерттеп ақпарат жинаған. Ақпаратты оңтайлы уақытта қолданып, өзіне керек ақпаратты алған. Бұл фркинигпен тоқтап қалмай авторизациялаудан өтпеген телефонды коммутаторды бұзу алаяқтығымен айналысқан. Яғни, телефондардың мекен жайларын ауыстырып шатасытыратын.

Әлеуметтік инженерия адамзатқа таныс болмай тұрып, қолданыста ие болатын. Оған дәлел, 1960 жылы Фрэнк Абанналэ Pan Am компаниясының жұмыскерлерін және басқа адамдарды өзі комерциялық ұшқыш екеніне сендірді. Фрэнк Абанналэ мектеп журналисті ретінде компанияның саясатын, процедураларын және өнеркәсіптің бағаланбас терминологияларын біліп алды. Алған ақпаратын және Pan Am ұшқыштарының киімін қолдана отырып әлем бойынша тегін ұшатын. Тегін ұшумен шектелмей, банктік үрдістер тұралы ақпаратты қолданып Pan Am компаниясының чектері арқылы ақша ұрлайтын.

Демек әлеуметтік инженерия 1970 жылдардың басында естілгенімен, бірақ сол уақытқа дейін қолданыста болған. Әлеуметтік инженерия 1970 жылдардан бастап, қазіргі таңда да актуалді мәселе болып табылады. Үстіде келтірілген фактілерге сүйене отырып, әлеуметтік инженерия болашақтада актуалді мәселе болып қала беретіндігіне күмән келтірмеймін. Себебі, адамзат қаншалықты дамығанымен машина емес, адамдардың

эмоцияларымен, мінез құлқымен оңтайлы уақытта дұрыс қолдана білсең қызықтыратын ақпаратты алу мүмкін болып табылады. Ал оған орай электронды құрылғылармен қолдана білу бұл ықтималдылықты 100% көтереді.

3 Әлеуметтік инженерия түсінігі

Әлеуметтік инженерия дегеніміз- социология, психология және алаяқтық әдістерді қолдану арқылы, ақпараттың негізгі қасиеттерін (конфиденциалдылығын (құпияланғандық), тұтастығын, қатынау қолайлығығың) бұзу арқылы қалаған мақсатына жету амалы. Әлеуметтік инженердің мақсаты - адам туралы жасырын ақпаратты немесе пайда алып келетін құпия ақпараттарды алаяқтық жолмен алу. Құпия ақпарат - бұл логин/ құпия сөз, жеке деректер, банк карталарының нөмірлері және қаржылық немесе беделді шығындарға алып келетін барлық нәрсе.

Көбінесе әлеуметтік инженерияны ақпаратқа заңсыз қол жеткізу амалы деп ойлайды, бірақ бұл толығымен шындық емес. Әлеуметтік инженерияны кей жағдайларда заңды түрде қолданады. Мысалы, қол жетімсіз нәтижелерге қол жеткізу немесе оң істерге алып келетін жағдайға адамдарды және топтарды програмаллау үшін қолданылады. Әрине қазіргі кезде әлеуметтік инженерияны көбінесе ғаламтор желісі арқылы құнды ақпараттарға қол жеткізу үшін қолданады, бірақ қазіргі замандық әлеуметтік инженерлер, әлеуметтік инженерияны жеке бизнесін үлкейту және нәтижелерін нығайту үшін қолданады. Бұған дәлел, әлемге есімдері әйгілі әлеуметтік инженерлер Дэвид Бэннон мен Питер Фостер өздерінін кіші кәсіпорындарын дамыту мақсатында әлеуметтік инженерияны қолданған.

3.2 Brain hack

Әлеуметтік инженерия түсінігі бізге хакинг ауқымынан келді. Хакер дегеніміз компьютердің кемшіліктерін анықтап , сол арқылы құпия ақпарат алатын адам. Хакер мен әлеуметтік инженерия арасындағы қатынас неде? Бір уақытта хакерлер әр жүйеде ең осал ол аппарат (машина) емес адам екенін түсінді. Адам машина секілді белгілі бір заңдылықтармен жұмыс істейді. Адам тарихындағы психология саласындағы және біреуге әсер ету механизмдерінің тәжірбиелері арқасында хакерлер машиналарды емес адамдарды бұза бастады. Мен бұны “brain hack” деп атаймын. Демек, хакер мен әлеуметтік инженер екеуі бір біріне өте ұқсас болып келеді. Анықтай кетсем хакер электронды машинаның кемшіліктерін, операциялық жүйе кемшіліктерін бұзады, ал әлеуметтік инженер адамдардың мінездерін зерттеп кемшіліктерін табу арқылы адамды бұзып керек ақпарат алады.

4 Әлеуметтік инженерия амалдары

Әлеуметтік инженерияның барлық әдістері когнитивті бұрмалануларға негізделген. Бұл мінез-құлық қателіктерін, әлеуметтік инженерлер тарапынан жасырын ақпаратты алуға бағытталған шабуыл жасау үшін пайдаланады, көбінесе жәбірленушінің келісімімен. Адамдардың эмоцияларының және мінез құлықтарының осалдылығын әлеуметтік инженерлер біліп, осалдылықтармен толыққанды қолданады.

Мысалы, компанияға бейтаныс адам кіріп, хабарландыру тақтасына, ресми тұрғыда жасалғанға өте ұқсас хабарландыру іледі. Хабарландыруда ғаламтор желісінің провайдерінің ұялы телефон нөмірі ауысқандығы тұралы ақпарат жазылған. Компания қызметкерлері хабарландырудағы нөмірге қоңырау шалған кезде, зиянкес өзін ғаламтор желісінің провайдері ретінде таныстырып, құпия ақпаратты алу үшін жұмыскердердің логиндері мен құпия сөздерін сұрауы арқылы компанияға тиесілі құпия ақпараттарды заңсыз жолмен алуы мүмкін.

Үстіде келтірілген мысалға сүйене отырып, адамның немесе қоғамдық топтардың когнитивті бұрмалануына бір ғана хабарландыру жеткілікті екенін байқауға болады. Бұл адамзаттың осалдылығын білдіреді.

Әлеуметтік инженерияның бірнеше амалдары бар. Бұл әдістер төмендегі тізімде көрсетілген.

- Претекстинг
- Фишинг
- Квид про кво
- Жолдағы алма
- Ақпараттарды ашық көздерден іздеу
- Трояндық вирус әдістері

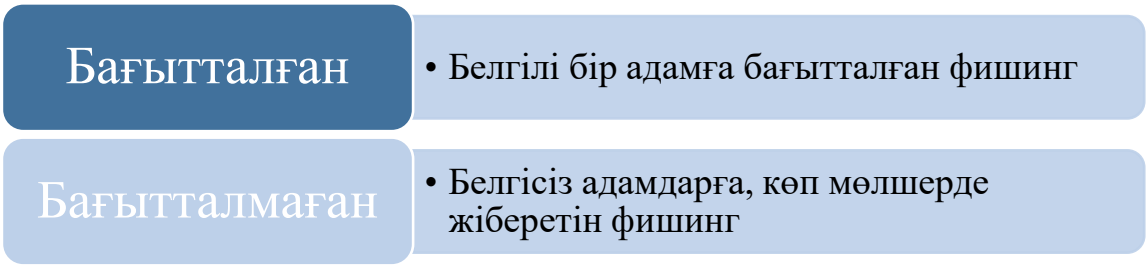
Бұл амалдарды қолдану үшін, зиянкесте алдымен зардап шегуші тұралы бастапқы ақпараттар болуы керек (аты жөні , атқаратын қызметі, жасап жатқан жобасының атауы, туылған жылы, күні туралы ақпарат). Кішігірім мысал ретінде, зиянкес алдымен шынайы жобаға байланысты сұрақтарын қойып , сеніміне кіргеннен кейін, оған өзін қызықтыратын құпия ақпараттарды біліп алу нәтижесінде сұрақтар қояды.

4.1 Фишинг

Фишинг – ғаламтор желісіндегі алаяқтық болып табылады. Фишингтің басты мақсаты, әр– түрлі жүйелерде авторизацияланған пайдаланушылардың құпия деректерін ұрлау болып табылады (логин, пароль, карталардың нөмірлері және тағыда басқа). Фишингтік шабуылдың басты әдісі болып, поштаға жалған хабарламаның келуі болып табылады. Келген хат ресми компанияның хатына немесе банктің ресми хатына ұқсас болып келеді. Ол хатта деректерді еңгізуге болатын бағандар немесе деректерді еңгізуге болатын бағандары бар web парақшасының сілтемесі болады. Бірақ қазіргі

таңда әлеуметтік желілердің дамығанымен қатар фишиингтік хабарландыруларды жіберу аланы өсуде. Пайдаланушылардың бұндай алаяқтыққа алдану себептері әр- түрлі бола алады. Мысалы, деректердің жоғалуы немесе жүйелердің бұзылуы ж/е т.б.

Фишингтік шабуылдар екіге бөлінеді



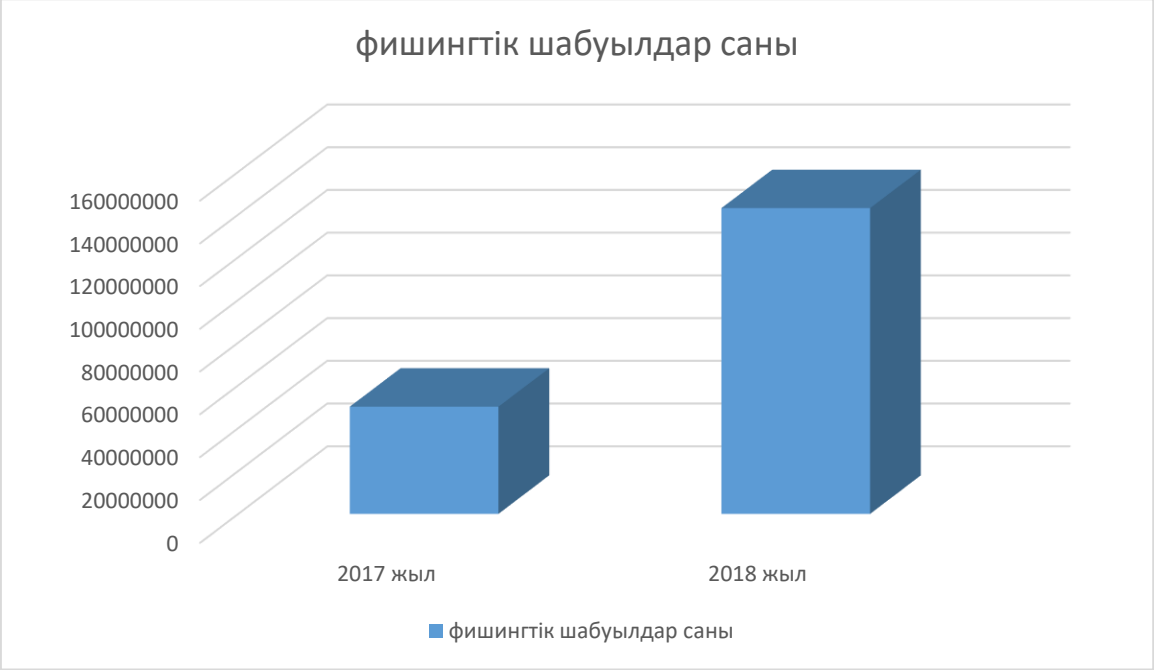
Бағытталған фишингтік шабуыл белгілі бір адамға жасалады. Фишингтің бұл түрі жүзеге асуы үшін зардап шегушіні толығымен зерттеу қажет. Зардап шегушінің қызығушылығы қандай, ұялы телефон маркасын, отыратын әлеуметтік жүйелері және т.б. Осы ақпараттарды қолдана отырып бағытталған шабуыл жасаған кезде, шабуылдың жүзеге асу ықтималдылығы жоғары болады.

Бағытталған фишингтік шабуылға мысал келтіретін болсам 2016 жылы болған «4127» атты топ Хиллари Клинтонның президенттік компаниясының мүшелеріне бағытталған фишингтік шабуыл жасалуы. Зиянкестер 1800 google электронды поштасына шабуыл жасап accounts-google.com доменін берген және пайдаланушыларды бопсалаған.

Бағытталмаған фишингтік шабуыл әдісінде фишингтік сілтемелер ірі, аттары әлемге әйгілі компаниялар атынан келеді. Бұл ауқымды фишингтік шабуылдар белгісіз көптеген пайдаланушыларға жіберіледі. Аты айтып тұрғандай фишинг балық аулауға ұқсас келеді. Фишингке біреу түседі, біреу түспейді. Сондықтан, фишингтің бағытталмаған түрі көп кездеседі.

Зерттеулердің көрсетуі бойынша 2018 жылы әлем бойынша компаниялардың 85 пайызына фишингтік шабуылдар жасалған. Бұл алдынғы жылмен салыстырғанда 65 пайызға көп.

Астыда көрсетілген диаграммада көрсетілгендей 2017 жылы шамамен 50000000 фишингтік хаттар жіберілген болса 2018 жылы шамамен 143000000 фишингтік хабарландырулар жіберілген.



CyberEdge компаниясының зертеулері бойынша 2015 жылы жасалған фишингтік шабуылдардың 71% жүзеге асты ал, 2016 жылы 76% көрсетті. Бұл көрсеткіш 2017 жылы 79% көтерілді.

Әлемге әйгілі фишингтік амалдар.

Астыда тангымал фишингтік амалдар жазылған :

- Әлемге әйгілі компаниялар брендттерінің есімдерін қолдану.
- Жасанды (өтірік) лотерея .
- Жалған антивирустар мен жалған қорғау бағдарламаларын қолдану.
- Телефон арқылы жасалатын фишинг (Вишинг).
- Жоқ сілтемелерді жіберу.

1 Әлемге әйгілі компаниялар брендттерінің есімдерін қолдану әдісі – бұл әдісте поштаға келген хат, әйгілі компаниялардан келген хабарландыру секілді келеді. Келген хабарландыруда сілтемелер болуы мүмкін. Сілтеме батырмасына басқан кезде, көз алдымызда компанияның ресми web парақшасына максималды ұқсас парақша ашылады. Хабарландыруда компания өткізген конкурстан жеңімпаз атандыңыз деген хабарлама немесе сіздің парақшаңыздың деректерін шұғыл түрде ауыстыру керек деген хаттар келуі мүмкін. Бұндай алаяқтықтар телефон арқылы да жүзеге асырыла алады.

2 Жасанды лотерея әдісі – бұл әдісте пайдаланушыға сіз конкурстан ұттыңыз деген хабарландыру келеді. Пайдаданушылардың алдану себебі, хат әлемге аты әйгілі компанияларға ұқсас фишингтік парақшадан келеді.

3 Жалған антивирустар мен жалған қорғау бағдарламаларын қолдану әдісі – бұндай алаяқтық бағдарламалар “scareware” деген есіммен белгілі. Бұл бағдарламалар антивирус секіліді көрінеді, бірақ атқару қызметі мүлдем керісінше. Scareware, пайдаланушыға әр- түрлі қауіптерді жалған түрде генерациялап жібереді және алаяқтық транзакцияларға бұрмалайды. Пайдаланушылар бұл жағдайға электронды пошта, онлайн хабарламалар,

социалді желілер, қалқымалы терезеден шығатын хабарландырулар арқылы соқтығысуы мүмкін.

4 Телефон арқылы жасалатын фишинг (Вишинг) бұлай аталуы себебі, фишингке ұқсас болып келеді. Фишингтің бір түрі деп айтса да болады. Бұл әдіс, алдын ала жазылып алынған дауыстар арқылы жасалады, сонда пайдаланушы бұл хабарлаушыны банктің немесе қалған IVR жүйелерінің ресми тұлғасы деп ойлайды. Әдетте пайдаланушыға фишинг парақшасы электронды поштаға келеді. Хатта пайдаланушы өзінің деректерін банк жұмыскеріне хабарласып өзгертуі керек немесе оны расстау керек деген хабарландыру келеді. Пйдаланушы жүйеге кіру үшін, пайдаланушыдан аутентификациядан өтуін талап етеді. Аутентификация PIN -ты және парольді енгізу арқылы жүзеге асырылады. Сондықтан алдын- ала жазылған жазба арқылы көптеген өзіне керек ақпаратты біліп алуға болады. Мысалға, әр адам алдын ала (құпия сөзіңізді өзгерту үшін 1 басыңыз, оператордың жауабын алу үшін 2-ні басыңыз) деген жазбаларды жазу мүмкін. Жазбаларды уақытысында қосып, автоматты түрде айтылатын сөздер ретінде көрсетуі мүмкін.

5 Жоқ сілтемелерді жіберу әдісі – келесі жолмен орындалады. Пайдаланушыға хабарландыру келеді. Хат жіберген зиянкестің есімі, пайдаланушыны қызықтыратындай болады. Хат ішіндегі сілтеме пайдаланушыны азғыртатындай болып келеді. Мысалы, “PayPal” денген сілтеме келеді,сілтеме “PayPal” ресми парақшасына ұқсас болып табылады, бірақ әр пайдаланушы бұл алаяқтықты байқамайды.

Бұл әдіске мысалы 2003 жылы болған оқиғаны келтірсем болады. 2003 жылы мыңдаған ebay пайдаланушыларына фишнгтік хат келеді. Хабарландыруда, пайдаланушылардың парақшалары бұзылғандығын жазады. Парқашаны қалыпты күйіне келтіру үшін, пайдаланушыларға карталарының деректерін қайта енгізуді талап еткен. Эксперттердің зерттеулері бойынша, сол шабуылдан кейін пайдаланушылар жалпы есеппен бірнеше миллион доллар көлеміндегі шығындарға тап болған.

Қазіргі кезде ақпаратты қорғау алдыға нық қадам жасады. Сонымен қоса, іздеу жүйелерінің әзірлеушілері де сәйкесінше қадамдар жасауда. Сондықтан, қазіргі кездегі жүйелердің көбісі фишингтік хаттарды және зиянкес парақшаларды анықтай алады. Анықталған хаттарды спамға салады. Антивирустар одан да жақсы қорғайды. Бірақ өкінішке орай, даму деген екі жақты құбылыс. Қорғаныс күшейген сайын, зиянкестерде әр түрлі жолдар ойлап табуда. Сондықтан, фишингтік шабуылдар әлі күнге дейін актуалды болып табылады, себебі хабарламалар және web парақшалар зиянкестің ойлаған уақытына сай қолданылса пайдаланушылардың алдануы әбден мүмкін.

Фишингке жасаған менің практикалық жұмысым. Алдымен фишингке айналатын ресми парақшаны таңдадым. Қазіргі кезде дүние жүзінің 2,5 млрд адамы қоғамдық жүйелерде отырады. Соның ішінде ВК қоғамдық жүйесінде айына 97 млн адам отырады. Қазақстанның өзінде ВК әлеуметтік жүйесіне 2

миллион активті падаланушы тіркелген. Үстіде келтірілген фактілерге сүйене отырып мен ВК қоғамдық жүйесін таңдадым. Келесі қадамда ВК қоғамдық жүйесін толығымен зерттедім. Күй келбетін, доменін және т.б.

Келесі қадамда SmartApe хостинг парақшасына тіркелдім. SmartApe хостингтік парақшаны тандаған себебім 14күн тегін қолдануға болады. FTP пайдаланушысы болдым. Ninite бағдарламаларды таратушы сайтынан Fille Zilla бағдарламасын орнаттым. Fille Zilla бағдарламасы тегін ашық FTP клиенттік бағдарлама болып табылады. Fille Zilla бағдарламасына хостинг парақшасындағы идентификациялау деректерін енгіздім. Хост адресін жазып, клиенттік бағдарламаға өз атымнан кірдім. Домендердің папкасына кіріп ВК парақшасының пішінінің скрипттерін Fille Zilla-ға (серверге) орнаттым. Түсінікті болу үшін Fille Zilla ол SmartApe парақшасымен байланысты. Енді вк-нің фишингтік парақшасы пайда болды. Оны хостинг парақшасы арқылы кіріп қарадым. Бірақ дегенмен фишингтің парақшасының сілтемесі, ресми вк парақшасынан мүлдем өзгеше. Бұл ақаулықты өзгерту мақсатында Freenom.com парақшасына кіріп фишингтік парақшанын сілтемесін vk01.ga ауыстырдым.

Енді вк қоғамдық жүйесінде авторизацияланған адамдардың ішінен кез келген адамды таңдаймыз. Таныс достарының біреуін таңдау дұрыс болып саналады. Себебі, таныс адамды зерттеуге уақыт кетірмейсің. Таныс емес адамға жіберуге болады. Бірақ бөтен адамға жіберсең, біріншіден ол адам немен қызығатынын білу керек. Екіншіден, ол адамның жеке құқығын бұзу деп саналады. Сондықтан, мен әрине бөтен адамға жібердім. Алдымен пайдаланушы немен қызығатының білдім. Пайдаланушы корей елімен толығымен қызығатының білдім. Корей тағамымен, корей киімдерімен, корей адамдарының түр келбеттерімен қызығатының анықтадым. Корей қыздарының түр келбеттеріне еліктейтінін анықтадым. Логикалық тұрғыдан ойлап қарасам, корейлердің түр келбетіне еліктесе, яғни корейлер секілді болғысы келеді. Ондай жағдайда өзіне қарап жүреді. Өзіне қарайтын адам болса, өзі тұралы адамдар не ойлайтынына қарайды.

Келесі қадамда, вк қоғамдық желісінің ресми парақшасына максималды ұқсас фишингтік парақша құрдым. Доменің ресми түріне ұқсас доменге ауыстырдым. Енді, құрылған фишингтік парақшасының сілтемесін жәбірленушіге жібердім. Фишигтік парақшаға өзінің деректерін енгізді. Деректермен кез келген заттар жасауға болады. Деректерді қолданып құпия ақпараттарды алуға, ақша талап етуге және т.б. алаяқтық іс-әрекеттер жасауға болады.

Фишингке жасаған зертеу жұмысымды талдаймын :

1 Алдымен, фишинг жасалынатын аумақты таңдаймыз.

2 Фишингке алданатын пайдаланушыларды таңдаймыз.

3 Пайдаланушыларды зерттейміз.

4 Бүкіл ақпаратты қолдана отырып, фишингтік парақшаны жүзеге асырамыз. Зардап шегушіге электронды пошта арқылы хабарландыру жібердім.

Адамдарды фишингтік парақшаларды айқындауға және фишингпен әр түрлі әдістермен қарсы тұруға үйретуге болады. Көптеген ірі компаниялар жұмыскерлердің шеберліктерін білу мақсатында симуляциялық фишингтік шабуылдар жүргізеді.

Фишингке қарсы қолданатын менің ұсынатын амалдарым:

1 Сайттың жеке дизайны. Бұл әдістің мәні пайдаланушы сайтқа кірген кезде сайттың фонын өзі таңдайды. Келесі реттерде кірген кезде сайт пайдаланушы таңдаған фонмен қосылады. Егер пайдаланушы сайтқа кірген кезде, фонды көрмесе немесе басқа фонды көрсе ол жалған сайттан дереу мезетте шығып, қауіпсіздік қызметтеріне хабарласу керек. Болжам бойынша зиянкес, зардап шегуші фонды таңдаған кезінде қасында болмаса, пайдаланушы таңдаған фонды біле алмайды.

2 Бір реттік құпия сөздер. Яғни қазіргі кезде, көптеген адамдар бір құпия сөзді бірнеше банктік карталарға қолданады. Бұндай құпия сөздерді зиянкестер біліп алатын жағдайда, зиянкес құпия сөзді өзі қалаған уақытында бірнеше рет қолдана алады. Ал бір реттік пароль кезінде, бір парольді бірнеше картаға емес, бір карта үшін әр түрлі құпия сөздерді қолданады. Яғни, пайдаланушы жаңадан кірген сайын жаңа құпия сөз енгізіп тұрады. Қорғанудың бұл әдісі сандар генераторлары арқылы жүзеге асырылады. Сандар генераторы әр түрлі құпия сөздерді бес он минут сайын өзгертіп тұрады. Пайдаланушы картаны енгізген кезде, өзінің генераторын іске қосып, генератордағы құпия сөзді енгізеді. Қазіргі кезде генераторлар әр түрлі пішімді, сондықтан ыңғайлылықпен мәселе туындамайды. Яғни ыңғайлы және ең бастысы қауіпсіз.

4.2 Претекстинг

Претекстинг бұл алдын ала ойластырылған, тәжірбиеленген әрекеттер жиынтығы. Нәтижесінде зардап шегуші кейбір ақпараттарды беруі мүмкін немесе зиянкес айтқан әрекеттерді жасауы мүмкін. Претекстинг әдісін қолдану алдында, зиянкесте зардап шегуші тұралы ақпараттар болуы тиіс. Қолдағы ақпараттар арқылы зиянкес өзінің шын жүзін зардап шегушіден жасырын ұстап қала алады.

Көбінесе бұл шабуыл түрі аудиожазбалар арқылы немесе Skype секілді әлеуметтік желілер арқылы жүзеге асырылады.

Бұл амалды қодану үшін, зиянкесте алдымен зардап шегушінің ақпараты болуы керек (аты жөнін, атқаратын қызметін, жасап жатқан жобасының атын, туылған жылы күні туралы ақпарат). Зиянкес алдымен шынайы жобаға байланысты сұрақтарын қойып , сеніміне кіргеннен кейін , оған өзін қызықтыратын құпия ақпараттарды біліп алу нәтижесінде сұрақтар қойады.

Претекстингке мысал, зиянкес зардап шегушіден белгілі бір соммадағы ақша алғысы келіп тұр. Қазіргі кезде адамның телефонын немесе қоғамдық жүйедегі парақшасын тауып алу оңай. Зиянкес зардап шегушінің парақшасын

және телефон нөмірін тауып алды. Ғаламтор желісінде адам туралы жүз пайыз ақпарат болмаса да, басты ақпараттар бар. Осы басты ақпаратты қолдана білетін әлеуметтік инженер өзіне қалаған ақпаратты немесе ақшаны қолына түсіре алады. Бұл ақпараттарға ұялы телефон нөмері, тұратын мекен жайы, жұмыс орны және тағы да басқа ақпараттар кіреді. Зиянкес ғаламтор желісі арқылы зардап шегушінің туған ағасы бар екенін тапты. Ағасының қоғамдық желідегі парақшасын тауып зерттеп, сол адам секілді ойлауға тырысады. Зардап шегушінің әлеуметтік желідегі парақшасын бұзып ағасы екеуінің хабарламаларын оқиды. Зиянкес зардап шегушіні хабарламалар арқылы зерттейді, зардап шегуші тұралы фактілерді тауып алады. Оған зардап шегушінің лақап аты, ортақ таныстарының есімдері, бірге баратын орындарының аттары және тағы да басқа. Осы жинаған ақпарат бойынша зиянкес жоспар құрады. Бұл жоспарда, зиянкес зардап шегушінің ағасының атынан түн ортасында хабарласып, біреу оны ұрып, ұялы телефоны мен ақша құжаттарын ұрлап алып кетті деп айтады. Бұл сөздерден кейін неге басқа нөмірден хабарласып тұрсын деген сұрақтар қойылмайды. Маңызды сәттердің бірі, зиянкес зардап шегушіге есімі арқылы емес, лақап атымен сәлемдесті. Зардап шегушінің лақап атын ағасы екеуінің хабарламаларынан біліп алды. Келесі қадамда зиянкес екеуіне ортақ таныс адамдардың есімдерін айтып, сол адамдармен бірге болғанын айтады. Бірақ ата аналарына айтпауын сұрайды, себебі атасының жүрегі ауыратынын ескертеді. Барлық ақпаратты хабарламалардан біліп алды. Осындай фактілерден кейін, сеніп қалған зардап шегушіден зиянкес таксиге ақша сұрайды және карточканың нөмерін береді. Карточка йесі хабарласуға ұялы телефонын берген адам деп айтады. Бұндай жасалған әрекеттерден кейін он адамның сегізі алданады.

Енді претекстингті талдайық, хакер осы жолы не қолданды ?

1 Өзіне керек адамның рөлін (ағасының) және сенімді оқиға ойлап тапты. Оқиғаны шынайы фактілермен толтырды. Атасы тұралы ақпарат, таныс адамдары тұралы ақпарат және лақап аты ж/е т.б.

2 Барлық оқиға тез уақытта айтылды. Әлеуметтік инженерлердің басты ережелерінің бірі, адамға ойлануға мұрша бермей, оны жұмыс істету. Бұл психологиялық әдіс назарды қадағалап ұстай білу әдісі деп аталады

3 Ен маңызды механизмдердің бірі қолданылды. Жаңашырлыққа қысым жасалды. Бұл қысым зардап шегушінің ағасы болғандықтан үршейе түсті.

Бұл оқиға өте оңай және сенгісіз көрінгенімен бұндай әдіске көптеген зардап шегушілер алданады. Себебі, адамның эмоциялары және мінез құлқының осалдалығы өз рөлін ойнайды. Бұған дәлел ретінде мен жасаған мысалды алсақ болады. Мен үстіде келтірілген оқиғаға ұқсас зерттеу жүргіздім.

Претекстинке жасаған мысалым:

- Алдымен зардап шегушіні таңдадым. Зардап шегуші ретінде Асхат есімді жігітті таңдадым.

- Әлеуметтік желілер арқылы туылған жылын, instagram желісін тауып алдым. Әлеуметтік желідегі достары арқылы электронды поштасының адресін біліп алдым.

- Электронды поштасына үстіде жасалған ВК әлеуметтік желісінің фишингтік парақшасынын сілтемесін жібердім. Сенімді көріну үшін ВК әлеуметтік желісінің әкімшілігінін атынан хабарландыру жібердім. Хабарландыруда: “ВК әлеуметтік желісіндегі парақшасы өз қызметін тоқтатты. Тоқтау себебі осы аккаунттан спам хабарландырулар таратылды. Парақшаны қайтадан бастапқы қалпына келтіру үшін астыдағы сілтеме бойынша өтіп, жаңадан логин және құпия сөз еңгізу керек”. Сенімділікті күшейту үшін қолтаңбаға ВК әлеуметтік желісінің белгішесін қойдым.

- ВК әлеуметтік желісінде досы екеуінің хабарландыруларын оқыдым. Оқу барысында тұратын мекен жайын, ортақ достарының есімдерін, бірге жиі баратын жерлерін, құрбысының есімін, ата анасы тұралы және т.б. ақпараттарды білдім.

- Келесі қадамда түнгі сағат 3:00-де хабарластым. Лақап есімі арқылы сәлемдесіп жиі баратын түнгі клубта барлық заттырын біреу ұрлап кеткенін айттым. Ортақ достарының есімдерін айтып хабарласқанда ұялы телефондарын алмағанын айттым. Құрбысы екеуі түнде қайта алмай тұрғанын жеткіздім. Бұл кездейсоқ адамның ұялы нөмірі екенін айтып, осы кісінің банктік картасына таксиге ақша салып жіберуін сұрадым. Келесі күн қайтарып беретініме сөз бердім.

- Зардап шегуші осындай алаяқтық іс- әрекеттерден кейін ақшаны банктік картаға 5 минут шамасында салып жіберді.

Претекстинг әдісінде адамның эмоциясына байланысты жасалғанына байланысты қарсы тұру қиын болып келеді. Дегенмен, Асхат өзінің мұқияттылығын танытқан кезде ВК парақшасынан келген хабарландыру жалған екенің көруі әбден мүмкін еді. Екіншіден, зиянкестің дауысы өзге болғандықтан досына қайта қоңырау шалу керек. Үшіншіден, тек екеулерін білетін сұрақ қойылуы тиіс.

Претекстингке қарсы тұру үшін, компания жұмыскерлері қоғамдық жүйелердегі өздерінің ақпараттарын азайтуы тиіс немесе ақпараттарына қол жеткізе алатын адамдар санын шектеу тиіс. Қазіргі кезде көптеген қоғамдық жүйелерде өз ақпараттарыңды жасырын ұстауға мүмкіндік бар. Дегенмен, екінші әдіс (шектеу) осал болып келеді. Себебі, ақпаратқа қол жеткізе алатын адам арқылы құпия ақпарат ағып кетуі мүмкін.

4.3 Кви про кво

Кви про кво әдісі – бұл әдісте зиянкес, пайдаланушыға электронды пошта немесе корпортивтік телефон арқылы хабарласады. Зиянкес пайдаланушыға өзін техникалық көмек жұмыскері ретінде таныстырып, техникалық ақаулар болғаның хабарлайды. Келесі қадамда ол пайдаланушыға ақауларды жою керек екенін айтады. Одан кейін зиянкес,

пайдаланушыны өз ыңғайына қарай қолданады. Мысалы, зиянды бағдарламаларды орнатуға немесе өзінің деректерін ашып беруге итермелейтін іс ірекеттер жасайды.

Кви про квоға жасаған зертеу жұмысым. Ең алдымен кви про кво әдісіне зерттеу жүргізу үшін пайдаланушыны таңдадым. Таңдаған жұмыскер IPSOS компаниясының бас бухгалтері. Еңді қызметкердің жұмыс орнын зерттедім. IPSOS компаниясы консалтингтік компания болып табылады. IPSOS компаниясы қазіргі кезде халықаралық компания болып табылады. IPSOS компаниясының басты мақсаты әріптестеріне зерттеу жұмыстарын өткізу. Ол анкета немесе сұрау түрінде болады. IPSOS компаниясының қазіргі әріптестерің зерттедім. Зерттеулер жүргізген кезде, IPSOS компаниясы Coca Cola, KFC, Monster компанияларынан тапсырыстар алған.

Келесі қадамда IPSOS компаниясының жұмыскеріне алдын ала дайындалған хабарландыру жібердім. Хабарландыруда өзімді техникалық қызмет көрсету маманы ретінде таныстырдым. Мен KFC компаниясының электронды поштасына ұқсас пошта құрып, IPSOS компаниясынын бас бухгалтеріне хабарландыру жібердім. Хабарландыру ішінде болашақта өткізетін сұрауларда өзгертулер бар деп жаздым. Өзгертулерді сілтеме арқылы көруге болатынын жаздым.

Сілтемеде өзім құраған өзгертілулер және зиян бағдарлама болды. Сілтеменің батырмасын басқан кезде винлок вирусы қосылып, экранды блоктады. Винлок вирусын винлобуайлдер бағдарламмасы арқылы құрдым. Енді IPSOS компаниясының бас бухгалтері ақаулықты шешу мақсатында мені шақырды. Мен вирусты өшіру үшін алдымен пайдаланушы идентифифкаторларын білу қажет екенін айттым. Келесі қадамда IPSOS компаниясының жұмыскері маған өзінің корпоративтік идентификаторларын айтты. Алынған идентификаторлармен мен кез келген товарды компания атынан сатып ала алатын болдым.

Енді кви про квоны талдаймын

1 Қызметкерге өзімді таныстырдым. Есінде мен қалдыратындай әрекет жасадым.

2 Қызметкер мені шақыру үшін әрекеттер жасадым. Вирус арқылы компьютерін бұздым.

3 Қызметкер өз қолымен маған идентификаторларын беру үшін әрекет жасадым.

4 Кви про кво жүзеге асты. Мен жұмыскердің вирусын жойдым (вирусты өзім еңгіздім). Жұмыскер маған өзінің идентификаторын берді.

Бас бухгалтер алдану себебі, адамға деген сенімділігі. Мен IPSOS компаниясының жұмыскері болғандықтан менен ондай алаяқтық күткен жоқ. Бұндай ақаулықтар адамның мінез құлқының ақаулықтары. Бас бухгалтердің жасаған қателігі идентификаторларын айтпауы тиіс еді.

Осындай ақаулықтарды алдын алу үшін қауіпсіздік саясаты қажет. Қазіргі кездегі компаниялардың 80%-да қауіпсіздік саясаты жоқ. Қауіпсіздік саясаты өте қажет зат болып табылады. Қауіпсіздік саясатында жұмыскер

өзін қалай ұстау керек екені жазылады. Бас бухгалтерге келсек ең басында қауіпсіздік саясатымен жұмысын орындаған кезде алдымен хабарландыру жіберушіні айқындап алу керек еді. Екіншіден, бұндай тақырыптағы хабарландырулар бас бухгалтерге келмеуі тиіс. Хабарландыру келген жағдайда белгілі жұмыскерге айтуы қажет еді. Дегенмен хабарландыруды ашқан жағдайда идентификаторларды ешкімге айтпау қажет. Техникалық қызмет көрсету жұмыскері болса да, жұмыскерге айтпай бас бухгалтер жеке енгізуі керек.

Кви про кво әдісіне компания қарсы тұру үшін, жұмыскерлерді жаңа жұмыскермен таныстыру қажет. Компанияда ақ тізім жасалуы керек, сонда тек авторизациядан өткен телефондар ғана қоңырау шалу мүмкіндігіне ие болады.

4.4 Трояндық вирус және жолдағы алма

Трояндық вирус – бұл әдіс пайдаланушының эмоцияларына негізделген. Мысалы, қорқыныш, қызығушылық таныту және тағы да басқа. Зиянкестің хатында антивирустың жаңартылуы, ақшалай ұтысқа кілт немесе жұмыскерге сыйлық болуы мүмкін. Шын мәнінде хабарламада зиян бағдарлама орналасқан. Пайдаланушы бағдарламаны қосқан кезде, бағдарлама компьютерден керек ақпараттарды ұрлайды.

Жолдағы алма әдісі трояндық вирусқа ұқсас келеді. Бірақ вирус физикалық тасымалдаушыларда болады(CD, флэш жинағыш және тағы да басқа). Зиянкес әдетте тасымалдауышты қол жетімді жерлерде сақтайды (көлік тұрақтары, асхана, жұмыс орындары, дәретхана және т.б.). Пайдаланушы тасымалдаушыға көңіл аудару үшін, тасымалдаушыға компания логотипін немесе басқа жазуларды жазу мүмкін. Мысалы, “сатылым тұралы деректер”, “жұмыскерлердің жалақысы”, “салық тұралы ақпарат” ж/е т.б.

Мысалы, зиянкес компания белгісі жабыстырылған диск тасымалдаушыны қол жетімді жерге тастап кетеді. Диск тасымалдаушыға 2012 жылғы жұмыскерлер жал ақысы тұралы ақпарат деп жазба жабыстырады. Жұмыскер дискті алып өз компьютеріне салуы мүмкін, себебі адамның қызушылығы ол мінез құлық осалдылығы. Зардап шегуші вирусы бар диск тасымалдаушыны компьютерге салған кезде вирус компьютерге енеді және зиянкес компьютерге қашықтықтан қол жеткізе алады. Зиянкес компьютерге немесе компьютерлік жүйеге зардап алып келе алады.

2016 жылы өткен зерттеулерге сай Иллинойс университетінің кампусынын жан жағына 297 флэш тасымалдаушы қойылған. Дискте вирус бағдарламалары болған. Зертеудің нәтижесінде 297 флэш тасымалдаушының 290-ы демек 98%-ы алынған. Ал 135 флэш тасымалдаушы вирусты жүзеге асырған.

Трояндық вирус әдісіне және жолдағы алма әдістеріне мысал-трояндық вирус әдісі, аты айтып тұрғандай трояндық вирустар арқылы

жүзеге асырылады. Трояндық вирустардың көптеген түрлері бар. Мысалы, қашықтықтан рұқсатсыз қатынас жасайтын, деректерді жоятын, деректерді жазатын, қауіпсіздікті сақтайтын бағдарламаларды өшіретін және т.б. Дипломдық жұмысымның, трояндық ат әдісінде қашықтықтан рұқсатсыз қатынас жасайтын вирусты қолдандым.

Ең алдымен зерттеу жұмысы болатын аумақты таңдадым. Мен таңдаған аумақ жастар кітапханасы. Жастар кітапханасының компьютерлік бөлімшесінде вирусы бар флэш тасымалдаушыны жұмыс стөлдің үстіне қойып кеттім.

Флэш тасымалдаушының ішінде қашықтықтан рұқсатсыз қатынас жасайтын вирусты еігіздім. Зардап шегуші ол вирус екенін анықтап қоймауы үшін оны суретке жабыстырып салдым. Ол үшін алдымен

1 Ең алдымен вирусты, суретті және байланысты файлдарды архивтадым

2 Енді блокнот бағдарламасын ашып «copy /b 1.jpg + 1.rar 2.jpg» деген кішігірім код жаздым. Бұл код вирус және вирусты тығатын сурет екеуін қосып 2.jpg атты сурет құрады.

3 Суретті bat форматында сақтап іске қостым. Қосқан кезде суреттін өзі ашылады. Бірақ қалған файлдар іске қосылады. Қосылған файлдарды диспетчер задач арқылы көрсе болады. Уретте қандай вирус бар екенін білу үшін оны архиватор арқылы ашу керек.

4 Бағдарлама дайын.

Келесі қадамда, зардап шегуші флэш тасымалдаушыны алып кетуін немесе кітапханада іске қосуын күттім. Зардап шегуші флэш тасымалдаушыны кітапханада өзінің ноутбугіне салды. Флэш тасымалдаушыда тек қана бір опера браузері болғандықтан оны іске қосқан жоқ. Қасындағы досы флэш тасымалдаушыны сұрап алды. Флэш тасымалдаушының ішіндегі вирусты іске қосты. Мен зардап шегушінің ноутбугімен толығымен басқара аламын. Вирус қосылған және вирус жазылып алынды деген ақпаратты алмады. Вирус білінбей С дискте жаңа папка ретінде сақталады.Вирус арқылы мен зардап шегушінің ноутбугімен басқара аламын. Бірақ ол үшін зардап шегуші ноутбугімен пайдаланбауы тиіс. Егер пайдаланушы активті болса, оның іс қимылдары бірінші нөмірлі орындалады. Сол үшін пайдаланушы ноутбукпен жұмыс істемей отырған кезде, электронды құралымен не істегің келеді соны істеуге болады.

Мен зардап шегушінің компьютеріне кіріп, вирустың тұрған жерін қарадым.

Тасымалды алма әдісінен қорғану амалдары.

- Бөтен адамның флэш тасымалдаушысын алмау тиіс
- Біреудін флэш тасымалдаушысын алған жағдайда, флэш тасымалдаушыны тазалау арқылы бастапқы қалпына келтіру керек.
- Тазартудан өтпей ашатын жағдайда, флэш тасымалдаушының ішіндегі бағдарламалар немесе фото, видео және т.б. виртуалды машина ішінде ашылуы тиіс. Вирус болған жағдайда виртуалды машинаны өшіріп, сонғы сақтау болған уақытқа қосамыз. Бұл шаралады жүргізбеген

жағдайдада, зиянкес тек виртуалды машинаны бұза алады. Компьютерге ешқандай қауіп төнбейді.

- Басқа компьютерлерде қосып тексеру. Яғни өзінің емес, мысалы комьютерлік клуб немесе кітапханадағы компьютерлерде тексеріп алу қажет.

Кері әлеуметтік инженерия – бұл әдіс пайдаланушы, зиянкеске өзі көмек сұрауға итермелейтін әдіс болып табылады. Кері әлеуметтік инженерия тұралы, пайдаланушы зиянкеске ақпаратты өзі берген кезде айтады. Бұл ойға қонымсыз болып көрінсе де, бірақ шын мәнісіне келгенде, техникалық немесе қоғамдық салада беделі бар адамдар, жиі пайдаланушылардың идентификаторлары және көптеген құпия ақпараттарын алады, себебі ешкім беделді адамдардаң күмәнданбайды. Мысалы, қолдау көрсету қызметкерлері, сізден ешқашан индентификаторларынызды немесе құпия сөзді сұрамайды. Бірақ көптеген пайдаланушылар өздерінің құпия ақпараттарын, мәселенің тез шешілу мақсатында береді. Демек, зиянкес пайдаланушыдан құпия ақпараттарын сұраған жоқ.

Кері қоғамдық инженерияға мысал : мысалда идентификаторларды қалай оңай алып алуға болатынын көрсетеді. Сізге системный администратор жексенбі күні сағат таңғы 8/00 қоңырау шалады. Сис админ /қазір бізде техникалық жұмыстар болып жатыр, қиын түсініксіз терминдер айтады, қазір келе аласыз ба сіздің компьютеріңізді ашу керек болып жатыр деп айтады. Сіз ішіңізден жексенбі күні таң атпай бір минуттық жұмыс үшін барып жүремін бе ? деп ойлайсыз. Тез арада, мәселені шешетін басқа жолдар бар ма? -деп сұрайсыз. Әрине бар, сіз маған идентификаторларынызды беріңіз (логин, құпия сөз) мен кіріп бүкіл мәселелерді шешемін, дүйсенбі күні келіп идентификаторларыңызды өзгерте аласыз деп айтады. Сіз ашық жүрекпен қуана қуана логин, құпия сөзіңізді системдік администраторға бересіз де ары қарай ұйықтайсыз. Сенгісіз, бірақ бұндай алаяқтыққа 70 пайыз адам түседі. Демек зиянкес 10 адамның нөмірлерін тауып, қоңырау шалса 6-7 адам өзінің логин, құпия сөздерін береді. Себептері оңай, хакер алдмен бәрін нашар тұрғыдан көрсетеді (жексенбі, таңғы сағат 8/00, тездетуліктің итермелеуі). Сіз ойланып баруға тура келеді деген шешімге келдіңіз, ал енді күтпеген жерден сізге келмейтін және мәселені оңай шешуге болатын нұсқа айтады. Әрине көп адамдар келіседі.

4.5 Ақпараттарды ашық көздерден іздеу

Ақпараттарды ашық көздерден іздеу әдісі – қоғамдық инженерияны қолдану үшін, тек психология саласындағы қабілет жеткіліксіз, қолдану үшін адам тұралы ақпаратты іздеу қабілетті де өте маңызды. Ақпаратты алудың жаңа түрлерінің бірі болып осы әдіс саналады. Ақпаратты көбінесе қоғамдық жүйелерден алады. Мысалы, livejournal, «Одноклассники», «ВКонтакте» секілді парақшаларда үлкен ауқымдағы ақпараттарын адамдар жасырмайды. Әдетте, адамадар қауіпсіздікке аса көңіл бөлмейді. Ақпараттарын қол жетімді жерде қалдырып, зиянкес онымен қолдана алады деп ойламайды.

Мысалға, Евгений Касперскидің баласының ұрлануын айтса болады. Зерттеулер көрсеткендей, зиянкестер баласының сабақ кестесін және үйге жүретін жолдарын қоғамдық жүйелерден біліп алған.

Қоғамдық жүйедегі ақпараттарын сырт көзден құпия ұстаған адамдар, ақпараттары зиянкестің қолына түспейтініне сенімді бола алмайды. Мысалы, бразильдік инженердің зерттеулері көрсеткендей, кез келген адамның досы болу үшін, тек 24 сағат жеткілікті. Зерттеулер кезінде Нельсон Новаес Нето жәбірленушіні таңдап, жәбірленушінің қасындағы адамның парақшасын құрды. Алдымен зиянкес, жәбірленушінің достарына дос болуды ұсынған. Парақшаны құрған уақыттан бастап жәбірленуші зиянкестің достығын қабылдауына дейінгі уақыт 7,5 сағат болған. Осылайша зиянкес, пайдаланушы сырт көзден сақтаған ақпараттарына қол жеткізді.

Менің ақпараттарды ашық көздерден іздеу әдісіне жасаған мысалым. Бірнеше ақпарат жинайтын адамды таңдадым. Таңдаған адамым, Сейлова Нургуль Абадулаевна. Аты- жөні белгілі. Сейлова Нургуль Абадулаевна 1979 жылы Қызылорда облысында дүниеге келген. 2001 жылы КазНИТУ жоғарғы оқу орнын бітірген. 2014 жылдан бастап КазНИТУ-нің ИИиТТ институтының ақпараттық қауіпсіздік кафедрасының жетекшісі. Келесі қадамда e-lib сайтында Нургуль Абадулаевна 53 публикация жасағанын көрдім. Публикациялар 2011 жылдан – 2017 жылдар арасында жүргізілген. Осы уақыт арасында жұмыс орны КазНИТУ деп белгіленген. Демек осы аралықта КазНИТУ-да жұмыс істеген деп ойлауға болады. Келесі қадамда, Қазақстанның ішкі істер министірлігінің сайтына кіріп тұратын мекен жайын білдім. Мкр.Мамыр 4, дом 295, кв 41. Көршісі Касымова Жубаныш Ишангалиева , Коптилеуова Дина Тургалиевна, Икранбеков Алмас Зубайрович. «Устройство защиты от несанкционированного доступа» атты проектте қатысты, АО Фонд Науки -дең грантты финансирование алды. Үйінің телефон нөмірі 87272396390. Ұялы телефоны 87073505038. Поштасы seilova_na@mail.ru. Каспи банкінің, каспиголд картасымен қолданады. Картаның соңғы сандары 5687.

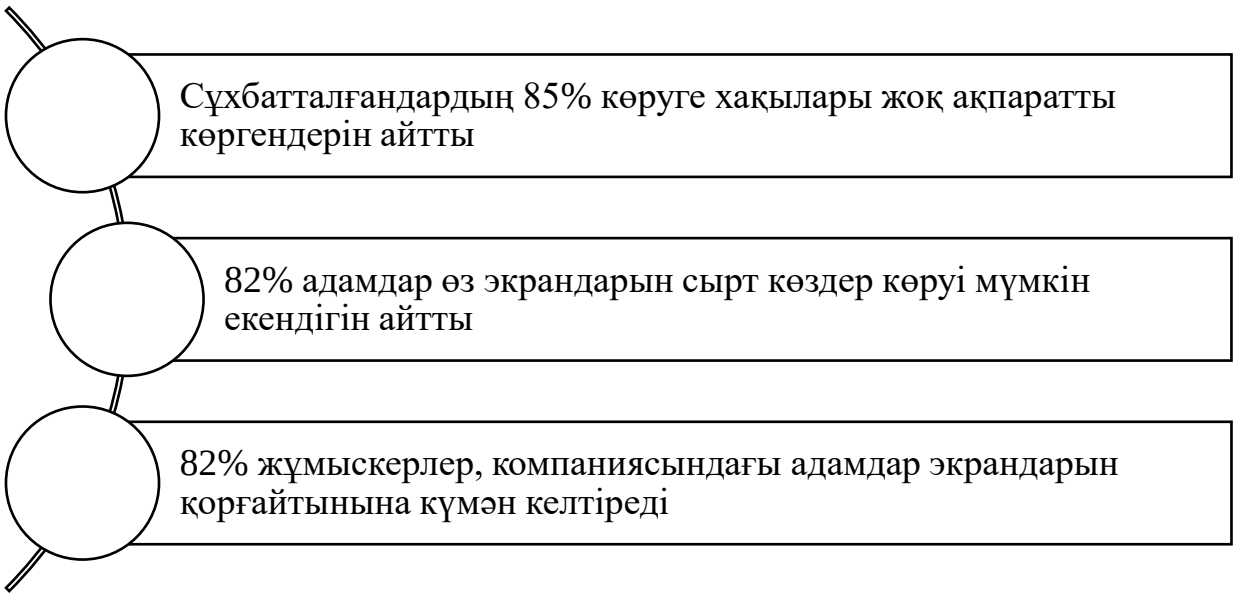
Әсер ету механизмдер әдісі – бұл әдіс социалді инженерлердің ең сүйікті және ақпаратты толық беретін түрлерінің бірі болып табылады. Бұл әдістің негізгі амалы, адамдардың психологиялық әлсіздігін қолдану арқылы керек ақпаратты алу. Мысалы, өзара ауысу амалы. Бұл амалдың өте көп түрлері бар. Біреуіне мысал келтірейін, сіз ұзын кезекте тұрсыз. Ен алдында ерте келген кісі тұр. Кісінің көңіл күйі түсіріңкі екенін байқадыңыз. Кезектің алдында тұрған кісіге келіп, шоколад ұсынасыз. Көңіл күйіңізді көтеру үшін деп айтасыз. Біраз уақыттан кейін, өтірік жүйкеніз тозып сағатқа жиі қарайсыз. Бір жерге кешігіп бара жатқандай кейіп танытасыз. Келесі қадамда, сіз шоколад берген кісі сізді байқап сізге өз кезегін береді. Бұл әдіс қауіпсіз әдістердің бірі болып табылады.

Әсер ету механизмдерінің тамашалығы, ол жеке адамға және топтарға да қолдана алуында.

Адамның эмоционалды күйімен басқару әдісі – қоғамдық инженерлерлердің қолданатың басты әдістерінің бірі болып табылады. Кездесулер жүргізген кезде немесе жай диалог жүргізген кезде, адамға әр түрлі эмоция бере алатын адам әңгімені басқарады. Зиянкестер бұл заңдылықты өте жақсы біледі және өкінішке орай кенінен қолданады. Ең көп кездесетіні, адамға аяушылық, жанашырлық немесе күнәлік сезімдерді сездіру. Көбінесе бұл амалдар іске асуы ең жоғары болып табылады. Мысалы, жолда бір кісі балама тамақ алып беру үшін ақшалай көмектесіп жібересіз бе ? деп сұрағанда бермесен бір түрлі сезім туындайды. Егер бөтен адам келіп, сізді әр түрлі эмоцияға баулайтын іс әрекеттер жасаса, бұл адамнан сескену керек. Бұндай әдіс өте оңай ашылады, ол үшін Eq-ні өсіру керек.

Йықтық серфинг әдісі – бұл әдіс аты айтып тұрғандай, адамның құпия ақпаратын артынан тұрып бақылау. Бұл әдіс көбінесе қоғамдық жерлерде кездеседі (кафе, парк, әуе-жай, торговый центр). Сондықтан құпия ақпараттарды немесе корпаративтік ақпараттарды қоғамдық жерлерде оқуға болмайды.

ИТ мамандарының қауіпсіздік тұралы зерттеулері ақ кітапта жазылған



5 Әлемге есімдері әйгілі социалді инженерлер

Кевин Митник

Әлемдегі ең әйгілі қоғамдық инженерлердің бірі болып Кевин Митник саналады. Әлемге атты әйгілі хакер және қоғамдық инженер бола тұра, Митник көптеген компьютерлік қауіпсіздік тақырыбындағы, әсіресе қоғамдық инженерияға көңіл бөлетін кітаптардың авторы. 2001 жылы «Исскуство обмана» атты Митниктің кітабы дүиеге келді. «Исскуство обмана» кітабында қоғамдық инженерияны шанайы өмірде қолданғаны тұралы жазылған. Кевин Митниктің айтуы бойынша құпия сөзді өтірік айту арқылы алу, компьютерді бұзу арқылы алғаннан оңай. Кевин Митник адал жолға түскен уақыттан бері әлеуметтік инженерия туралы бірнеше кітап жазған. Оларға мысалы, «Исскуство обмана», «Исскуство вторжения», «Призрак в проводах» және т.б.

Бадир ағайындылары

Бұл екі ағайындылар Мушид және Шадир Бадир туыла соқыр болғанымен, әлемге танымал қоғамдық инженерлер болып табылады. Бадир ағайындылары 1990 жылы Израильде алаяқтықтың бірнеше ірі схемаларын құрып, оларды жүзеге асырған. Интервью кезінде Бадир ағайындыларының айтуы бойынша жүйелік шабуылдардан тек қана телефон, ноутбук немесе басқа электронды құралдарды қолданбайтын адам ғана толық қорғанған. Ағайындылар ұялы телефондардың жүйелерінің интерференциалды тондарын естіген үшін абақтыда отырған. Олар шет елге ұзақ уақыт бойы қоңырауды тегін шалып жүрген.

Архангель

Архангель әйгілі компьютерлік хакер және ағылшын тіліндегі Phrack Magazine атты журналдың қауіпсіздік консультанты. Архангель қоғамдық инженерияның әдістерін көрсетіп, бірнеше жүздеген адамдарды алдаған.

Басқа әлеуметтік инженерлер

Аттары танымал Фрэнк Абигнейл, Дэвид Бэннон, Питер Фостер және Стивен Джей Рассел атты қоғамдық инженрлер бар.

Үстіде жазылған әлемге есімдері әйгілі әлеуметтік инженерлердің өмірбаяндарын, берген кеңестерін оқи отырып әлеуметтік инженерия қазіргі таңда, шыққан кезінен бастап өз актуалдылығын жоғалтпағанын көрдім. Әйгілі әлеуметтік инженерлердің қолданған амалдарын зерттей келе, әлеуметтік инженерияны тек зиян жағынан емес, өз ісінді өркендету мақсатында қолдануға мүмкін екенін көруге болады.

6 Әлеуметтік инженериядан қорғану немесе алдын алу жолдары

Компаниялардың компьютерлік жүйелерінің осалдылығын зерттейтін орындар, компьютерлік жүйелерге әлеуметтік инженерия арқылы кіру әдістері әр дайым 100% болғанын айтады. Ақпаратты қорғау технологиялары бұл әдісті қиындата түседі. Бірақ әлеуметтік инженерия мәселесін шешу үшін немесе алдын алу үшін ақпараттың қауіпсіздік технологияларымен, ақпаратты қорғау саясатының бірігуі керек. Ақпаратты қорғау саясатында жұмыскерлер өздерін қалай ұстау керек екені тұралы жазылуы тиіс. Сонымен қатар саясатта жұмыскерлерді дайындау тұралы ақпарат болуы тиіс.

Әлеуметтік инженериядан қорғанудың негізгі түрі болып жұмыскерлерді дайындау болып табылады. Барлық жұмыскерлер өздерінің немесе компанияның деректері кез келген уақытта сырт көзге ағып кетуі мүмкін екенін және ол зиянкестерден қалай қорғану керек екенін білу керек. Одан орай әр қызметкерлерде, жұмыс орнына және лауазымына байланысты қандай тақырыптарға қалай сөйлесу керек екені тұралы нұсқаулар болуы тиіс. Нұсқауда жұмыскер қандай ақпаратты техникалық қызмет көрсету орталығының жұмыскеріне беруге болады және компания жұмыскеріне өзіне керек ақпарат алу үшін қандай деректерді беру керек екені жазылуы тиіс. Қоғамдық инженерлер шабуылдарды жұмыскерлердің шынайылығына, еріншектілігіне, адамгершілігіне сүйене жасайды. Бұл шабуылдардан қорғану қиын, себебі жұмыскерлер зиянкес оны алдағысы келіп тұрғанын түсінбейді. Қоғамдық инженерлер, қарапайым зиянкестер секілді ақша, құпия ақпарат немесе компанияның IT ресурстарын алуға көздейді. Бұл шабыулдардан қорғану үшін, алаяқтықтың түр түрін зерттеу керек, зиянкеске қандай ақпарат керек екенін түсіну керек, оны зерттеу керек. Зиянкес ісін жүзеге асырса, шығын қанша болатынын білу керек. Бұл ақпараттардың бәрін білсе, қауіпсіздік саясатына өзгертулер енгізіп, компанияны қорғауға болады.

Ақпаратты анализден өткізу – ақпаратты толығымен анализдеу керек. Құпия болып келетін ақпаратты идентификациялау және оны әлеуметтік инженерияға осалдылығын тексеру. Құпия ақпаратты қауіпсіздік жүйелері сәтсіздікке ұшыраған кезде зерттеу.

Хатамалар құру – ақпаратты өңдеу, сақтау тұралы қауіпсіздік саясатын және протоколдарды құру.

Event Test- уақыттан тыс қауіпсіздік тесттерін өткізу.

Қалдықтармен басқару- Қоқыс қораптарына тек құпия емес ақпаратты тастау керек. Қоқыс кораптары құлыптармен құлталуы тиіс. Құлыптардың кілттері тек тазалау жұмыскерлерінде болуы тиіс. Қоқыстардың тұрған орындары айқындалуы тиіс, яғни зиянкес қоқыстан құпия ақпаратты алғысы келетін жағдайда қоқыс қорабынын тұрған орны үлкен рөл атқарады. Мысалы, қорап офис ортасында тұрған жағдайда, оған қол жеткізу қиын болып табылады, себебі адамдарда сұрақтар пайда болуы мүмкін.

Бұдан орай, келесі ережелерді бөліп көрсетуге болады

- Қызметкерлердің кіретін идентификаторлары компанияның меншігі болып табылады. Барлық қызметкерлерге жұмыс орнынан берілген логин және құпия сөздер компания меншігі екенін және оны басқа мақсатта қолдануға(жеке пошта үшін, web парақшаларға кіруге және т.б.) болмайтынын немесе оны үшінші жаққа берілмеу керек екені айқын түсіндірілу керек. Мысалға, кейбір жұмыскерлер демалысқа шыққан кезде өзінің идентификаиорларын әріптесіне қалдырып кетеді.

Қызметкерлерге жиі қауіпсіздік шараларын ұлғайту мақсатында қауіпсіздік саясаты оқылуы керек. Бұндай шараларды өткізу, компания қызметкерлеріне актуалді қоғамдық инженерия әдістерін біліп жүруіне алып келеді. Қоғамдық инженерия әдісін білді деген сөз, шабуылдан 50 пайызға қорғану деген сөз.

- Қызметкерлердің қол астында қауіпсіздік ережелер және нұсқаулықтар болуы тиіс. Нұсқаулықтарда жұмыскер әр- түрлі жағдайлар туындаған кезде, не істеу керек екені жазылу тиіс. Мысалы нұсқаулықта, үшінші адам құпия ақпаратты сұраған кезде не істеу немесе қай жерге хабарласу керек екені тұралы ақпарат жазылуы мүмкін. Бұндай шаралар, ақпараттың ағып кетуінен сақтауға көмектеседі.

- Қызметкерлердің компьютерлерінде актуальді антивирустық бағдарламалар болуы тиіс. Қызметкерлердің компьютерлеріне одан орай брэндмауерлер орнату қажет.

- Копманияның корпоративтік жүйесінде қауіптілікті анықтау және шешу жүйелері болуы керек. Құпия ақпараттардың ағып кетпеуін қадағалайтын жүйелер орнату қажет. Бұның бәрі фитиновтық шабуылдардаң қорғайды.

- Барлық қызметкерлер келген клиенттермен қалай сөйлесу керек екені тұралы ақпарат алуы тиіс. Келген кісінің кім екенің анықтаудың нақты ережелері болуы тиіс. Келген кісілердің қасында әр дайым компания қызметкерлері жүруі тиіс. Егер қызметкер компания ішінен бөтен кісіні көрсе, ережелер бойынша қызығушылық таныту керек. Кісі бұл жерде қандай мақсатпен жүр екенін және оның қасындағы компания жұмыскері қайда деген сұрақтар қойылуы тиіс. Қажет жағдайда қызметкер, бөтен адам тұралы ақпаратты қаіпсіздік қызметкерлеріне айтуы керек.

- Барынша қызметкерлердің жүйедегі хақыларын азайту керек. Мысалы, қызметкерлерге web парақшаларына кіруді бөгеу және сыртқы ташығыштарды қолдануға рұқсат бермеу керек. Себебі, қызметкер ғаламтор желісінен фишингтік парақшаларды ұстамаса және сыртқы тасығыштар арқылы трояндық вирустарды компьютерге тасымаса, өзінің идентификаторларын жоғалту ықтималдылығы күрт түседі. Үстідегі бүкіл ережелерге сүйенсек ең мықты қорғаныс, ол жұмыскерлерді үйрету болып табылады. Әр жұмыскер, ережені бұзу жауапкершіліктен босатпайтынын білуі қажет. Әр қызметкер жеке ақпараттарының ағып кету қауіпін білу керек және оған қалай қарсы тұру керек екенің білу керек, себебі жүйенің ең осал бөлігі ол адам.

Қоғамдық инженерлердің шабуылын қалай білуге болады

Астыда қоғамдық инженерлердің амалдары жазылған

1. Өзін басқа қызметкер ретінде немесе жаңа қызметкер түрінде таныстырып, көмек сұрау.
2. Өзін тасымалдаушы компанияның қызметкері немесе әріптес компания қызметкері ретінде таныстыру
3. Өзін басқарушылардың бірі ретінде таныстыру
4. Өзін қауіпсіздік бағдарламалардың немесе компанияға сай бағдарламалардың жұмыскері ретінде таныстырып, жаңартуларды орнату мақсатымен хабарласу
5. Өзін техникалық қызмет көрсету орталығының қызметкері ретінде таныстырып, көмек көрсету және алдын ала шығатын қателерді енгізу. Қателердің енгізу себебі, сол қателерді түзеп сенімге кіру
6. Сенімге кіру мақсатында компания ішіндегі таныс сөздерді, терминдерді қолдану.
7. Вирустарды немесе трояндық жылқыларды хабарландыруға қоса жіберу
8. Жалған pop-up терезесін жіберу. Бұл терезе идентификаторларын қайта теруге өтініш білдіреді.
9. Парақшаға тіркелсеніз ұтыс аласыз деген жалған хаттар жіберу
10. Жұмыскер басып отырған батырмаларды өз компьютеріне немесе кейлогинггбағдарламасына жазу
11. Сыртқы тасымалдағыштарды көзге көрінетін жерлерде тастап кету
12. Құжаттарды немесе папкаларды компанияның пошта бөліміне тастап кету
13. Құжатты локальді адреске жіберуді өтіну
14. Зиянкес өзінің дауысын өзгерту, жұмыскер оны өз әріптесі деп ойлау үшін

Қауіптерді классификациялау

Телефонмен байланысты қауіптер

Телефон қазіргі күнге дейін компания ішінде немесе компания аралық коммуникация түрі болып табылады және қоғамдық инженерлерде көп қолданысқа ие. Телефон арқылы адамның түрін көре алмаудың себебінен, зиянкес өзін әріптес, бастық немесе конфиденциалды ақпаратқа қолы жетімді кез келген адам ретінде өзін таныстыра алады. Зиянкес, көбінесе өз өтінішін жұмыскер орындауға тиіс болатындай сұрайды, әсіресе өтініші оңай көрінгенде. Телефон арқылы ақша ұрлаудың басқа да түрлері әйгілі. Ұтысты қайта қайтару, конкурстан жеңіпаз атану немесе жақын адамдардың келеңсіз жағдайға түсіп, тез арада ақша сұрау тұралы смс немесе қоңырау келуі мүмкін.

Қауіпсіздікті сақтау шаралары бұндай смс-терге скептикалық көз қараспен қарауды ұсынады және келесі принциптерді ұстануға шақырады.

- Хабарласып тұрған адамның тұлғасын тексеру
- Нөмерді анықтау қызметтерімен қолдану

- СМС- тегі таныс емес сілтемелерді елемеу
- Электронды пошта арқылы келетін қауіп қатерлер

Көптеген қызметкерлерге күн сайын корпоративтік немесе өздерінің электронды пошталарына, күн сайын он немесе жүздеген хабарландырулар келеді. Әрине бұндай ауқымдағы хаттардың бәріне тиісті көңіл аудару мүмкін емес. Бұл шабуылды жасауға үлкен көмек. Көптеген жүйенің пайдаланушылары бұндай хабарландыруларды өңдеуде қауіпті ешнәрсе көрмейді. Пайдаланушылар бұны құжаттарды бірінші папкадан екінші папкаға ауыстырудың электронды аналогы деп көреді. Зиянкес пайдаланушыға оңай сұрау жіберген кезде, пайдаланушы ойланбастан сұрауды жүзеге асырады, себебі сұраудан ешқандай қауіп көрмейді. Хабарландыруларда сілтемелер болуы мүмкін. Сілтемелер, пайдаланушы компанияның құпия ақпаратын жарыққа шығаратын іс-қимылдар жасайды.

Көптеген қауіпсіздік жүйелері, авторизациядан өтпеген пайдаланушылар корпартивтік жүйеге кірмеуін бақылайды. Егер пайдаланушы, зиянкес жіберген сілтеме бастырмасын басса, корпаративтік жүйеге трояндық вирусын кіргізеді. Вирус, компанияның көптеген қауіпсіздік жүйелерінен өтіп кетуге мүмкіндік алады. Қалған қауіптер секілді, электронды поштаны қорғау үшін, келген хабарландыруларға скептикалық тұрғыдан қарау керек. Бұл тұрғыдан қарау үшін, қауіпсіздік саясатына бірнеше өзгертулер еңгізу керек. Бұл еңгізулер астыда көрсетілген

- Құжаттарға қосылып келген вложениялар
- Құжаттардағы сілтемелер
- Компанияның ішінен келген хатта, жеке немесе корпоративтік ақпараттар сұралса
- Компанияның сыртынаң келген хатта, жеке немесе корпоративтік ақпараттар сұралса

Бір сәтте хабарландырулармен ауысуға арналған қызметтерді қолдану кезіндегі қауіптер

Бір сәтте хаттармен ауысу қызметі жаңа әдіс болып саналғанмен, қазіргі кезде корпоративтік пайдаланушылар арасында әйгілі болып кетті. Бұл әдістің тездігі және оңайлығы, зиянкестердің шабуылына үлкен мүмкіндіктер береді. Пайдаланушы бұл қызметті, телефондық жүйе ретінде көріп, қауіпті бағдарламалармен байланыстырмайды. Сондықтан бұл әдіс қауіпті болып табылады.

ҚОРЫТЫНДЫ

Бұл дипломдық жұмыста әлеуметтік инженерияны зерттедім. Әлеуметтік инженерияны зерттегенімнің себебі қазіргі кезде әлеуметтік инженерия өте актуалді мәселе болып табылады. Әлеуметтік инженерия атты мәселені шешу немесе оны алдын алу үшін, әлеуметтік инженерия не екенін зерттедім. Әлеуметтік инженерияның амалдырын зерттеп, обьект және субьекттерін көрсеттім. Амалдардың әр қайсысына жеке- жеке практикалық жұмыстар жасадым. Осы практикалық жұмыстардың арқасында зиянкес қалай алаяқтық жасайтының және зардап шегуші неге алаяқтыққа түсетінін атап өттім. Зардап шегуші тек қана жеке адам емес, орта және үлкен компаниялар зардап шегуші рөлінде болуы мүмкін екенің көрсеттім. Әлеуметтік инженерия мәселесінен қорғану немесе алдын алу мақсатында, эксперттердің жазған кеңестерін оқып, тұжырымдамалар жасадым. Әлеуметтік инженерияның кейбір амалдарынан қорғану мақсатында, өзім бірнеше алдын алу әдістерін ойлап таптым. Ойлап тапқан амалдарды түбегейлі қарастырып, жүзеге асырылуын зерттедім. Әлемге аты әйгілі әлеуметтік инженерлердің оқиғаларын талдап, айтқан кеңестерін талқыға алдым. Толықтай кеткенде әлеуметтік инженерияны толығымен не екенің зерттедім. Себебі, ескертілген адам- қорғалған адам.

Алдыма қойылған мақсатты орындау үшін :

- Әлеуметтік инженерия түсінігімен таныстым
- Әлеуметтік инженерия кесіріне қазіргі кезде қаншама зардап шегуші тап болатының көрсеттім
- Әлеуметтік инженерия амалдарын зерттеп, практикалық жұмыстар жасадым
- Қазіргі кезде әлеуметтік инженерия актуалді мәселе екенің практикалық жүзінде дәлелдедім
- Әлеуметтік инженерия мәселесіне қарсы тұру жолдарын қарасытырдым
- Әлеуметтік инженерия мәселесіне қарсы тұру амалдарын ойлап таптым

Алдыма қойылған мақсаттарымды жүзеге асырдым. Оған қоса әлеуметтік инженерия тұралы толық ақпаратты “Исскуство обмана” “Исскуство вторжения”, “Социальная инженерия и социальные хакеры” атты кітаптарды зерттеп оқу арқылы алдым. Әйгілі әлеуметтік инженерлердің сөздері мен кеңестерінің ықтималдылығы мен жұмыс істеуін қарастырдым. Қорытындылай келсем, әлеуметтік инженерия қазіргі кезде өте актуалді мәселе болып табылады. Әлеуметтік инженерия мәселесіне қарсы тұру үшін бұл дипломдық жұмыспен қоса тағы да үстіде келтірілген кітаптарды зерттеу керек. Себебі, ескертілген адам- қарулы адам.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1 Кевин Митник, Искусство обмана / Компания АйТи; 2004.

2 Кузнецов М.В. Социальная инженерия и социальные хакеры/ СПб.: БХВ-Петербург,2007.

3 Кевин Митник.. Искусство вторжения: Компания АйТи; 2004..

4 Социальная инженерия //Электронды мәлімет көзі. Элек.журн. EFSOL жүйе интеграциясы 2017. Мәліметке қол жеткізу : https://narfu.ru /agtu /www . agtu.ru

5 Социальная инженерия //Электронды мәлімет көзі. Элек.журн. Ярослав Бабин 2018. Мәліметке қол жеткізу : https://xakep.ru

6 Фишинг-атаки //Электронды мәлімет көзі. Элек.парақ. Владимир Безмалый 2008. Мәліметке қол жеткізу : https://www.osp.ru

7 Как взломать человека //Электронды мәлімет көзі. Элек.парақ. COSSA агентілігі 2017. Мәліметке қол жеткізу : https://www.cossa.ru

8 Технология взлома человека //Электронды мәлімет көзі. Элек.журн. Никита Артемов 2017. Мәліметке қол жеткізу : https://medium.com

9 Социальная инженерия как метод взлома человека //Электронды мәлімет көзі. Элек.журн. Habr 2018. Мәліметке қол жеткізу : https://habr.com

10 Social Engineering //Электронды мәлімет көзі. Элек.журн. Imperva 2018. Мәліметке қол жеткізу : https://www.imperva.com

11 What is Social Engineering //Электронды мәлімет көзі. Элек.парақ. Robert Ikovly 2018. Мәліметке қол жеткізу : https://www.webroot.com

12 Social Engineering //Электронды мәлімет көзі. Элек.журн. Кевин Бивер2017. Мәліметке қол жеткізу : https://searchsecurity. Techtarget . com

13 More than one in 10 employees fall for social engineering attacks //Электронды мәлімет көзі. Элек.журн. Warrick Ashford 2018. Мәліметке қол жеткізу : https://www.computerweekly.com

14 Кристофер Хаднаджи Unmasking the Social Engineer: The Human Element of Security// By SPACED,2014.

15 Шарон Конхеди Social Engineering in IT Security: Tools, Tactics, and Techniques// ABC-CLIO,2014.

16 Social Engineering //Электронды мәлімет көзі. Элек.журн. Джефф Биккерс 2019. Мәліметке қол жеткізу : https://www.social-engineer.com/

17 Phishing //Электронды мәлімет көзі. Элек.парақ. Phishing inc 2019. Мәліметке қол жеткізу : http://www.phishing.org

18 Phishing //Электронды мәлімет көзі. Элек.журн. Imperva 2018. Мәліметке қол жеткізу : https://www.imperva.com

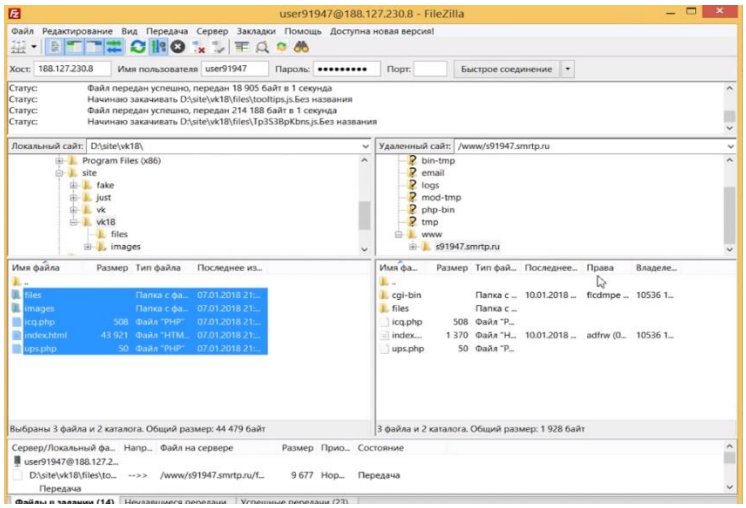
19 Уил Аллсопп Unauthorised Access: Physical Penetration Testing For IT Security Teams // A John Wiley and Sons, Ltd., Publication 2009.

20 Кристофер Хаднаджи, Мишел Финчер Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails //Gannett Company 2015.

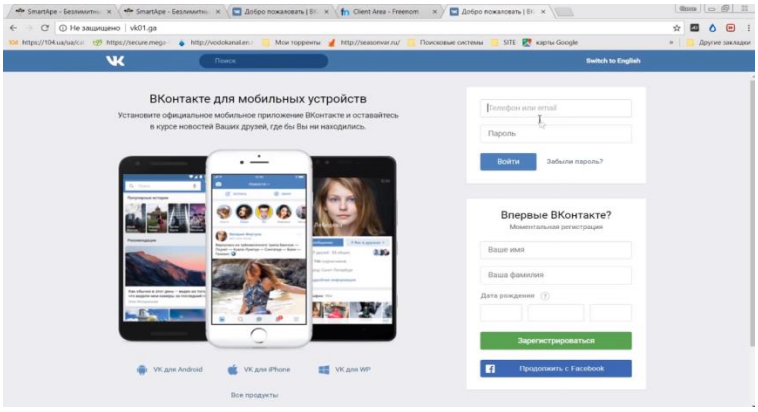
21 Социальная инженерия: Quid Pro Quo атаки //Электронды мәлімет көзі. Элек.журн. М Салман Надим 2015. Мәліметке қол жеткізу : https://blog.mailfence.com
22 5 Types of Social Engineering Attacks //Электронды мәлімет көзі. Элек.журн. KATIE THORNTON 2018. Мәліметке қол жеткізу : https://www.datto.com

ҚОСЫМША А

1- сурет. FTP пайдаланушысы ретінде тіркелу

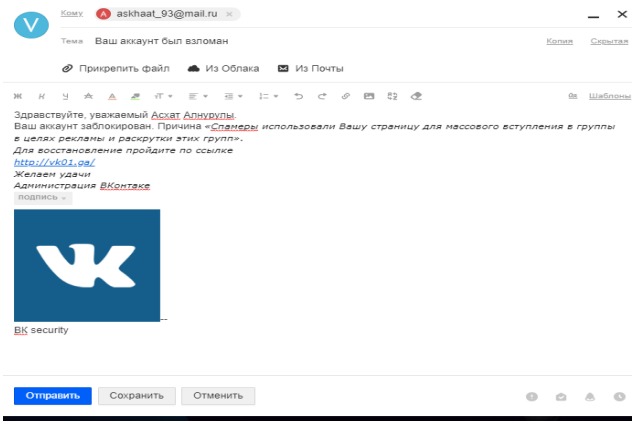


2- сурет. ВК парақшасынын келбетін, www папкасына орнаттым.



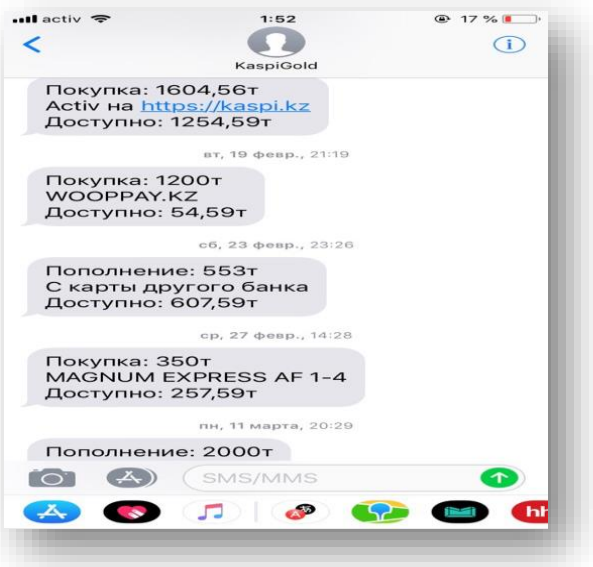
3- сурет. Вк парақшасына фишинг дайын.

ҚОСЫМША В



4-сурет. Зардап шегушіге фишингтік хабарландыру жібердім.

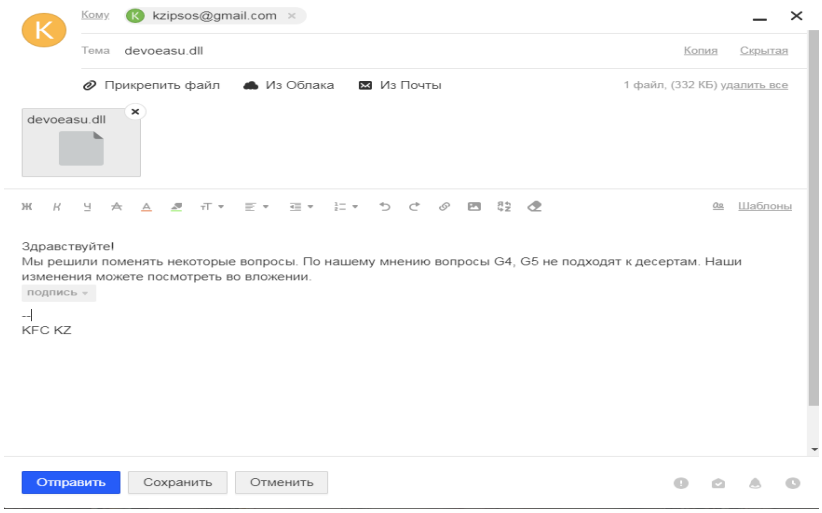
5-сурет. Зардап шегушінін қоғамдық жүйесін зерттедім.



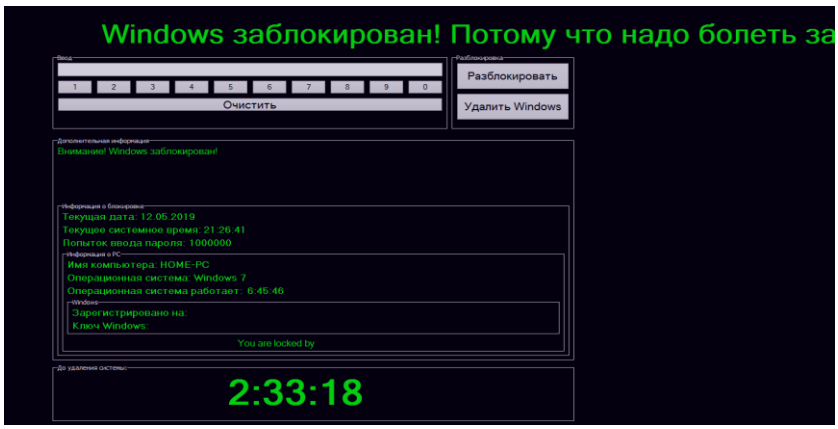
6-сурет. Зардап шегуші, әлеуметтік инженерияға тап болды.

ҚОСЫМША С

7- сурет. Винлок вирусын құрдым.

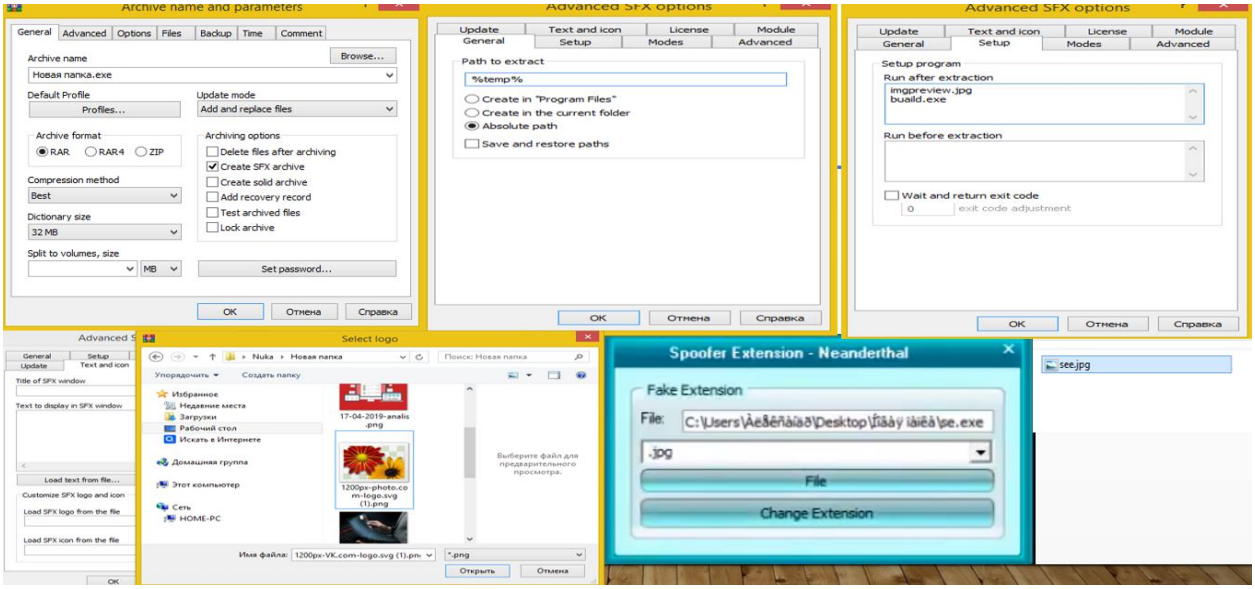


8- сурет. Компания бухгалтеріне вирус жібердім.

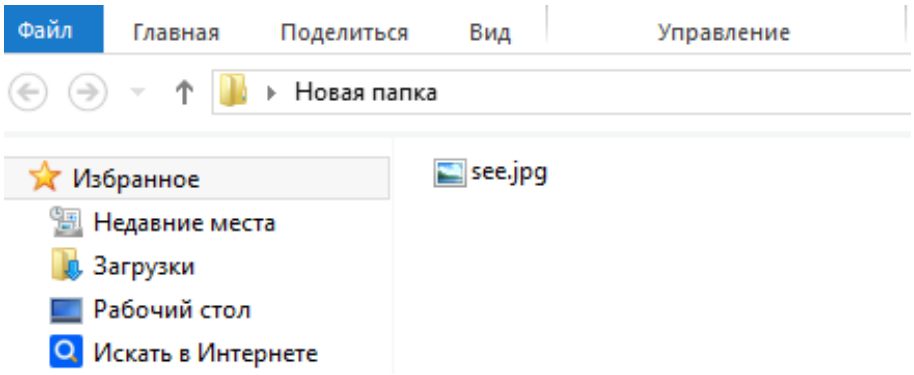


9- сурет. Вирус іске қосылды.

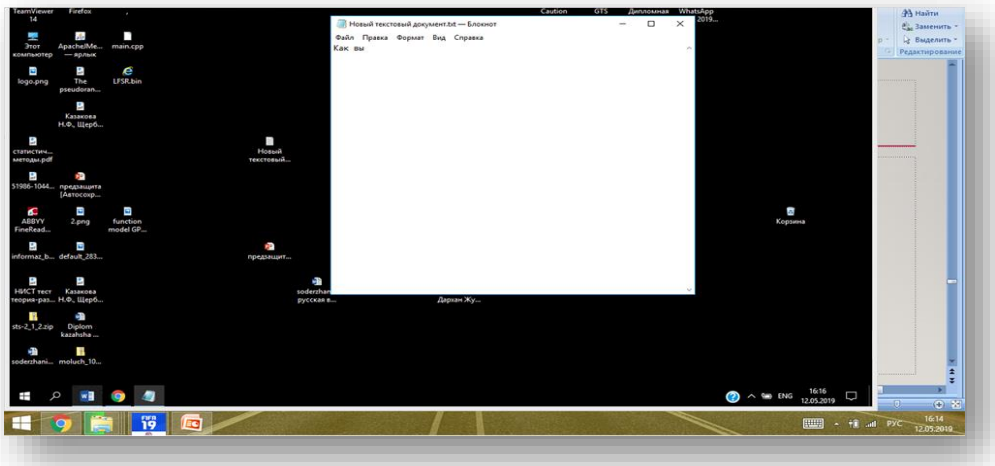
ҚОСЫМША D



10- сурет. Вирусты суретке жабыстырдым.

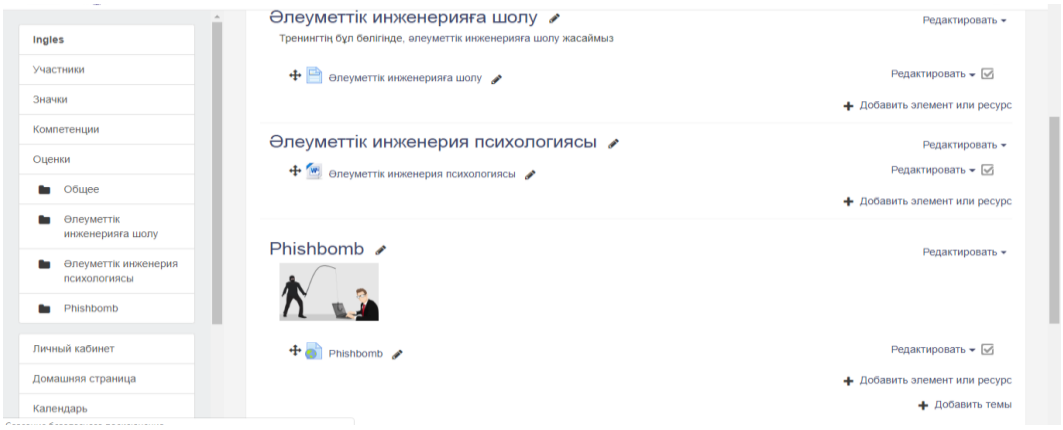


11- сурет. Вирус дайын.

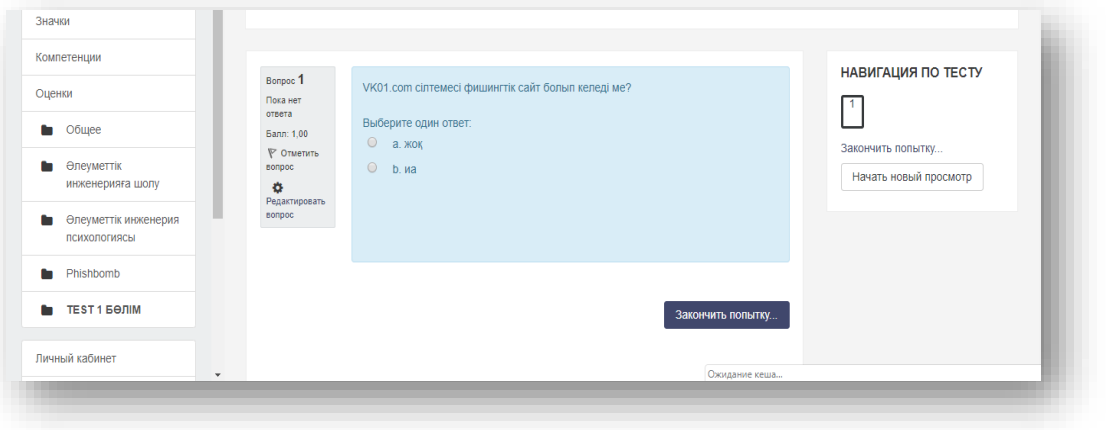


12-сурет. Қашықтықтан басқару вирусы іске қосылды.

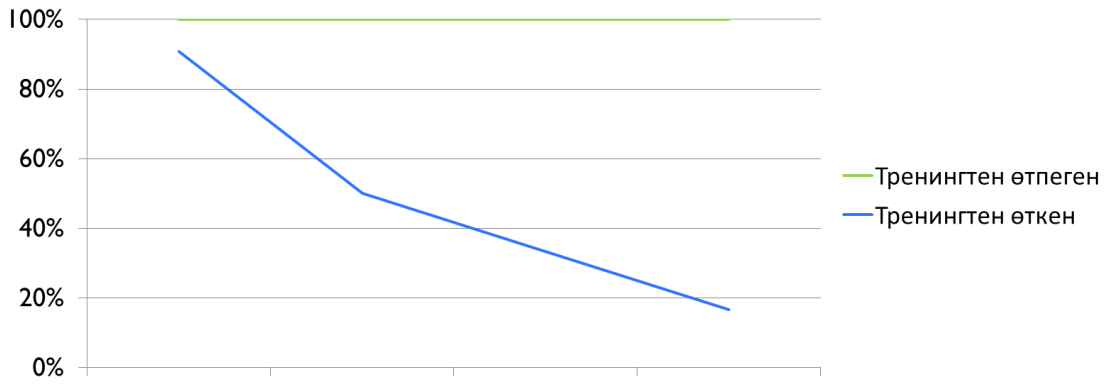
ҚОСЫМША Е



13- сурет. Әлеуметтік инженерияға қарсы тұру үшін жасалған тренинг.



14-сурет. Әлеуметтік инженерияға қарсы тұру үшін жасалған тренинг.



15-сурет. Тренингтен өткенен кейінгі жетістік.