УДК 004.056
DOI: 10.31673/2409-7292.2022.011626

Ганченко М.І.

ЛЮДСЬКИЙ ПСИХОЛОГІЧНИЙ ТА БІОМЕТРИЧНИЙ ФАКТОР У РОЗВИТКУ ТА ВИКОРИСТАННІ МЕТОДІВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ У МИРНИЙ ТА ВОЄННИЙ ЧАС

Предметом вивчення в даній статті є процес впливу соціальних інженерів на людей шляхом маніпулювання свідомістю, емоціями, почуттями без та з використанням сучасних інформаційних технологій обробки та імітації біологічних характеристик людства як у мирний так і військовий час**. Метою та завданнями** є: розгляд існуючих методів соціальної інженерії таких як: фішинг, троян, претекстинг, watering hole, бейтінг, quid pro quo, переслідування, зворотня соціальна інженерія під призмою людських почуттів: наївності, неуважності, жадібності, довірливості, цікавості, приналежності, страху; розгляд сучасних технологій: підробки почерку - алгоритм «My Text in your Handwriting», підміни голосу - сервіс Descript's Ovrlab, штучного діалогу - додаток Replika та заміни лиця - технологія Deep Fake, котрі можуть стати у пригоді шахраям для досягнення власних цілей щодо отримання конфіденційних даних та здійснення подальших атак на їх основі, а також маніпулювання свідомістю щодо реального сприйняття подій у військовий час. Використовуваними **методами** є: психологічний та соціоогічний метод проведення досліджень, такий як спостереження, методи соціальної інженерії, методи прогнозування на основі аналізу та висновків щодо розвитку тенденцій у майбутньому. Отримані такі **результати.** Створені асоціації методів соціальної інженерії з почуттями, на які спрямований той чи інший психологічний вплив соціального інженера. Визначений потенціал використання технологій, що розвиваються, з методами соціальної інженерії, для здійснення більш ефективних та витонченіших атак з урахуванням улюблених ефектів зловмисників: поспіху, несподіванки, спантеличення, викликання почуття жалю, тривоги, бурхливої радості і так далі. Оцінено можливість виникнення загроз стосовно проведення процедур автентифікації та авторизації користувачів за біометричними даними на основі розглянутих сучасних технологій імітації біометричних даних людства: почерку, голосу, лиця. Наукова новизна отриманих результатів дослідження полягає в наступному: доведено важливість та необхідність пильного ставлення до конфіденційної інформації, котру люди поширюють про себе у будь-яких аспектах свого соціального життя; визначено основні почуття на яких грають соціальні інженери для досягнення власних цілей та отримання вигоди; зазначено потенціал розвитку сучасних технологій імітації біометричних даних людей у ефективності здійснення атак методами соціальної інженерії, доведено ефективність використання засобів та методів соціальної інженерії під час ведення інформаційних війн за для впливу на нестійкий психологічний стан.

Ключові слова: соціальна інженерія; сучасні технології; конфіденційні дані; біометричні дані; психологічний вплив, війна.

Вступ

На сьогоднішній день поширені два основні підходи у сфері кіберзлочинності: використання сучасних технологій та соціальна інженерія. [1] Соціальна інженерія (social engineering) або «атака на людину» - це сукупність психологічних і соціальних прийомів, методів та технологій, які дозволяють отримати конфіденційну інформацію. [3]

Одним з популярних та головних видів зброї для кіберзлочинців залишаються методи соціальної інженерії. Тому що атаки з використанням даного підходу є високоефективними та недорогими. [2] У свою чергу, це дозволяє розширити спектр дії атак, зробити їх більш різноманітними та застосувати для реалізації нові сучасні технології. І сьогодні як ніколи, такі рішення мають успіх у веденні інформаційної війни, поширенні фейків та дезінформації населення, як допоміжного руйнівного психологічного фронту до основного - військового.

Глобальне поширення та занурення методів соціальної інженерії у повсякденне життя базується на принципі, що люди завжди були і залишаються найслабшою ланкою у захисті інформації. [1] І почуття – це те, на чому грають шахраї, особливо під час гібридної війни. Коли психологічний стан населення є найбільш хитким та вразливим.

Також виникають хвилювання щодо можливості реалізації загроз спрямованих на викрадення та незаконе використання біометричних даних людства. Сучасні технології сприяють розвитку і таких можливостей для зловмисників. Адже, настане час, коли кожному з нас заведуть цифровий профіль, і не за горами створення кіберособистості. А високі технології, що розвиваються, такі як: Інтернет речі, мобільні технології і хмарні розрахунки лише сприятимуть у все більш витонченішій діяльності кіберзлочинців. [17]

Тож дана стаття спрямована на розгляд людських психологічних та біологічних характеристик і їх роль у кібератаках методами соціальної інженерії та сучасними технологіями. Метою та завданнями є: розгляд існуючих методів соціальної інженерії таких як: фішинг, троян, претекстинг, watering hole, бейтінг, quid pro quo, пересліування, зворотня соціальна інженерія під призмою людських почуттів: наївності, неуважності, жадібності, довірливості, цікавості, приналежності, страху; розгляд сучасних технологій: підробки почерку - алгоритм «My Text in your Handwriting», підміни голосу - сервіс Descript's Ovrlab, штучного діалогу - додаток Replika та заміни лиця - техологія Deep Fake, котрі можуть стати у пригоді шахраям для досягнення власних цілей щодо отримання конфіденційних даних та здійснення подальших атак на їх основі, а також маніпулювання свідомістю щодо реального сприйняття подій у військовий час.

Сучасні методи соціальної інженерії (психологічний фактор).

Основою соціальної інженерії є психологія, а злочинці знають на що потрібно натиснути для отримання бажаного результату. [4] Саме на такій техніці базуються впливи на свідомість та підсвідомість, які призводять до необхідного рішення зі сторони жертви на користь атакуючого. [6] Розуміння цього аспекту є важливим етапом у побудові концепцій протидії та захитсу від атак даного виду. А питання безпеки персональних та конфіденційних даних є ключовим для кожного користувача інформаційних технологій. Саме тому, за тиждень, як згодом виявилось, до повномаштабного вторгенення Російької Федерції на територію України, що розпочалось 24 лютого 2022 року, було проведено статистичний збір інформації серед населення різного віку. Опитування містило 19 запитань розділених на 4 тематики:

1. Рівень обізнаності населення. Розділ містив 3 запитання загального характеру та визначав рівень ознайомленості населення різного віку з питанням соціальної інженерї.
2. Вплив соціальних інженерів на особистість. Розділ містив 11 запитань та визначав можливість впливу методів соціальної інженерії на собистість. Вивчалась ймовірність впливу наступних: претекстинг (питання 2-3), фішинг (питання 3-5), троянська програма (питання 5-6), бейтінг (питання 7-8), quid pro quo (питання 9), переслідування (питання 10), зворотня соціальна інженерія (питання 11).
3. Ставлення до розвитку сучасних інформаційних технологій. Розділ містив 3 запитання та визначав особисте ставлення опитуваних до певного виду поширених інформаційних технологій.
4. Висновок. Розділ містив 2 запитання, що формували висновок до пройденого опитування з рекомендаціями для перегляду ставлення населення до поширюваної особистої інформації в мережі.

Проведене соціологічне дослідження мало на меті визначити обізнаність та вразивість населення до дій соціальних інженерів. Тож і кожен з розглянутих надалі методів асоціюється з почуттям, на яке спрямований той чи інший психологічний вплив, з наступним статистичним відображенням результату.

Перший розділ опитування дозволив зрозуміти хто та наскільки обізнаний з поняттям «соціальна інженерія». Зведені дані за віком опитуванних містяться у табл.1. Відтак з 65-ти опитаних було виділено три вікові категорії: до 16-ти років (дитина, підліток); 16-59 років (людина працездатного віку); після 60-ти (літня особа); і рівень обізнаності серед більшості відповідно до віку та за варіантом відповіді виділений у таблиці сірим кольором. Тож данні свідчать про те, що більша частина населення – 26 осіб, знайома з поняттям «соціальна інженерія» та можуть його пояснити, окрім того значна частина – 35 осіб, розуміє методи які використовує для реалізації дане поняття.

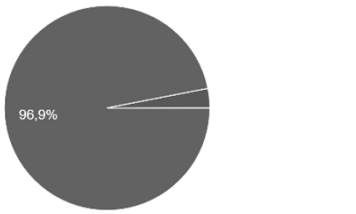
Наступним етапом в дослідженні посідає визначення місця методів соціальної інженерії як в повсякденному житті так і під час інформаційних війн у період ведення бойових дій. Для цього було визначено наявність акаунтів у соціальних мережах, їх доступність, відкритість щодо ведення сторінок та розповсюдження персональної інформації для

визначення можливості здійснення впливу соціального інженера на особистість. Результати опитування подані на діаграмах 1-3.

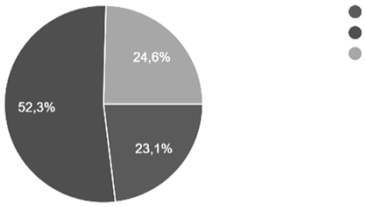
Таблиця 1.

Обізнаність у темі відповідно до віку опитуваного

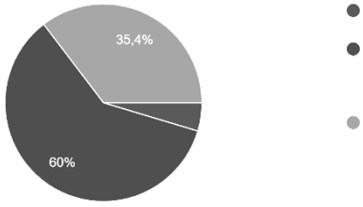
Питання і варіанти відповідей / Вік	До 16-ти років	16-59 років	Після 60-ти років
Питання 1. Вкажіть Ваш вік			
Кількість осіб, шт.	9	53	2
Питання 2. Чи знайомі Ви з терміном «Соціальна інженерія»			
Так, можу пояснити	-	26	-
Термін знайомий, та пояснити не можу	5	14	1
Ні	4	13	1
Питання 3. Чи знайомі Ви з наступними поняттями: фішинг, претекстинг, спам, бейтінг, переслідування?			
Так, можу пояснити кожне з понять	-	18	-
Терміни знайомі, можу пояснити деякі з них	4	30	1
Терміни знайомі, та пояснити не зможу	3	3	-
Ні	2	2	1



Діаграма 1. Розділ 2. Вплив соціальних інженерів на Вашу особистість. Питання 1. Чи маєте Ви акаунти у соціальних мережах та месенджерах?



Діаграма 2. Розділ 2. Вплив соціальних інженерів на Вашу особистість. Питання 2. Ваші акаунти є загальнодоступними (ввдкриті для загалу) чи приватними (відкриті для певного кола осіб)?



Діаграма 3. Розділ 2. Вплив соціальних інженерів на Вашу особистість. Питання 3. Чи поширюєте Ви приватну або конфіденційну інформацію (ПІБ, домашню адресу, номери телефонів, місця вашого перебування, навчання, роботи, дані банківських карток, паролі і т.д.) про себе на сайтах, у соціальних мережах і пабліках?

Дані свідчать про те, що 96,9% з 65-ти опитаних ведуть соціальні мережі, і більша половина – 52,3% мають приватні акаунти, та лише менша частка - 35,4% поширюють мінімально необхідну інформацію. Тому доцільно зазначити що більша частина опитаних не сильно переймаються станом захищеності своєї конфіденційної інформації і власноруч надають її для ознайомлення як знайомим (якщо акаунт приватний), так і невідомим особам (у випадку відкритого акаунту).

Тож розглядаючи надалі кожен з методів, було визначено його особливості, приклади використання, способи і ймовірність впливу на особу.

1. Фішинг - почуття: неуважність.

Метод збору інформації користувача для авторизації. [3] Спроба отримання конфіденційної інформації (імена користувчів, паролі, данні банківських карток, номера телефонів) шляхом маскування під відомі організації, бренди, магазини, банки та їх представників, задля виклику довіри щодо дійсності, справжності та серйозності. Атака здійснюється з використанням електронної пошти або sms-розсилки, куди надсилається лист з пропозицією перейти за посиланням. [7] Усе зазначене дійство супроводжується поспіхом та обмеженням часу на виконання з боку користувача. Це спричиняє вихід людини з рівноваги, подальше прийняття неправильних та необдуманих рішень. У результаті відбувається перехід на підроблений зловмисником сайт для вводу даних, необхідних для авторизації користувача. Таким чином конфіденційні дані стають доступними та відомими шахраю. [7]

Тож фішинг спрямований на керування діями потерпілого базуючись на наївності та неуважності останнього.

Питання 3-5 розділу 2 були спрямовані на визначення впливу фішингу на особистість. І результати наступні – діаграми 3-5.

Діаграма 4. Розділ 2. Вплив соціальних інженерів на Вашу особистість. Питання 4. Чи перевіряєте Ви посилання (URL-адреси) перед тим, як перейти за ними?

Діаграма 5. Розділ 2. Вплив соціальних інженерів на Вашу особистість. Питання 5. Як Ви реагуєте на повідомлення з наступним вмістом: "швидкий прибуток", "виграш", "натисни на картинку", "дай відповідь на лист", "відкрий документ"?

Відповіді свідчать про те, що 60% поширюють великий обсяг конфіденційної інформації, яка переважає необхідність для коректного функціонування сайтів чи надання послуг. Половина учасників опитування зазначили, що перевіряють джерела від яких отримують електронні адреси, тим не менш 32,8% періодично нехтують подібним аспектом, а 17,2% взагалі зневажають безпекою при переході за посиланням. Задовільним результатом у 83,1% щодо питання реакції на повідомлення-приманки є байдужість користувачів до подібних листів та вкладень. Але важливим у понятті ефективності фішингу є не кількість проігнорованих повідомлень, а збір метричних даних: скільки людей видаляє листи подібного змісту не читаючи, скільки прочитали але нічого не зробили, скільки прочитали але повідомили у відповідні служби, а також скільки відкрили вкладення та перейшли за посиланням. Тож небезпека у можливості потрапити на гачок зловмисника, котрий використовує фішинг залишається, що наглядно демонструється під час час війни 2022 року.

У зазначений період є сильно розповсюдженні фішингові атаки з використанням прикладних листів для ніби-то пітвердження даних, за для розблокування електронної поштової скриньки. Вимагається протягом короткого терміну перейти за посиланням та підтвердити облікові дані, в зворотньому напрямку скриня буде видалена безповоротньо. [17]

Також використовується шахрайська схема з виплатами грошової допомоги під час воєнного стану через розсилку SMS-повідомлень з посиланням на ресурс, де можна подати заявку на отримання допомоги. Для цього потрібно ввести персональні дані та номер

банківської картки для зарахування коштів. Вказані такого роду конфіденційна інформація на підозрілому ресурсі автоматично передається шахраям, після чого кошти з карток привласнюються. [17] Злочинці також намагаються викрадати дані платіжних карток використовуючи тематику грошової допомоги від ООН та країн ЄС імітуючи сторінки телеканалів ТСН та Україна24 у соціальній мережі Facebook. Пропонується взяти участь в опитуванні з наданням персональної інформації та здійсненням платежу, перейшовши за посиланням для отримання допомоги. Як результат – скомпрометовані дані платіжної картки. [17]

Розсилка небезпечних листів із тематикою «Кібератака» здійснюється ніби-то від імені CERT-UA – Урядової команди реагування на комп'ютерні надзвичайні події України, що діє при Держспецзв'язку. Листи містять шкідливе вкладення у вигляді захищеного паролем RAR-архіву «UkrScanner.rar». [17]

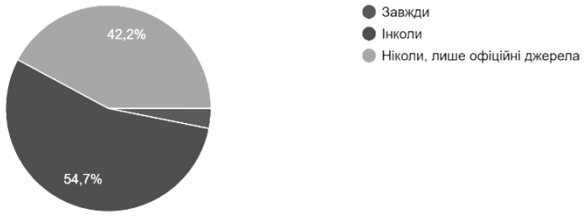
Електронні листи, що розсилаються ніби-то від Міністерства освіти і науки України з темою «Нова програма для запису в журнал», містять посиання на програму та пароль на архів, у разі відкриття якого відбувається викрадення персональних даних, завантаження і запуск виконуваних файлів та здійснення знімків екрану. [17]

2. Троянська програма – почуття: жадібність.

Метод викрадення даних, що має на меті маскування шкідливого програмного забезпечення – віруса, та впровадження його на пристрій жертви.[3] Зараження здійснюється через поштові повідомлення-приманки, які натякають на швидкий прибуток, виграш і спонукають здійснити певну дію: перейти за посиланням, відкрити документ, нанисnути на картинку, відповісти на лист. В результаті, користувач отримує вірус, що викрадає необхідні зловмиснику дані.

Як і попередній метод - спрямований на наївність, яка підсилена бажанням швидкого заробітку.

Питання 5-6 розділу 2 визначали ймовірність зараження пристроїв троянськими програмами, результати – діаграми 5-6.



Діаграма 6. Розділ 2. Вплив соціальних інженерів на Вашу особистість. Питання 6. Чи часто Ви завантажуєте ігри, музику, програми, додатки з невідомих, непідтверджених, незахищених, неофіційних джерел?

Дані з діаграми 5 вказують на те, що лише 1.5% виконають дії вказані у зловмисному повідомлені без будь-яких сумнівів та підозр. Та нажаль більше половини – 54,7% наражають себе на небезпеку встановлення шкідливого програмного коду, використовуючи для завантаження розважального контенту незахищені, невідомі чи неофіційні джерела.

У військовий час таке нехтування зову грає на руку злвмисникам, оскільки широко користовуються рекламні банери, розміщені на сайтах, чи файли-приманки з гучними заголовками: «довідка.zip», «лист справедливості.xlsx», «хімічна атака.xls», «Указ Президента України №576/22 про безпрецедентні заходи безпеки», «Військові на Азовсталі.xls», «Втрати-1001.docx», «заборгованість по зарплаті.xls». Такі файли містять шкідливий програмний код, запуск якого призводить до встановлення і запуску шкідливого ПЗ, котре, в свою чергу, забезпечує викрадення автентифікаційних та інших даних з інтернет-браузерів, клієнтів, криптовалютних гаманців, менеджерів паролів, месенджерів, ігрових програм тощо. [17]

3. Претекстинг – почуття: довірливість.

Метод що базується на сценарії з метою підвищення ймовірності залучення жертви. Даний вид впливу полягає у виклику почуття довіри до соціального інженера, котрий може

виступити у ролі вашого знайомого, друга, начальника, члена сім'ї.[3] Для правдоподібності шахрай на момент атаки уже володіє деякою правдивою інформацією, котру повідомляє, щоб увійти в довіру, зблизитись або ввести людину у знервований чи стан переживання, та дізнатись ще більше необхідних даних. Претекстинг засвідчує, що люди схильні довіряти, коли мова йде про знайоме, близьке, рідне, підсилене емоційним забарвленням.

Не обійшов інформаційну війну і даний метод у сукупності з фішингом, оскільки розповсюджуються фейки від імені Служби безпеки України з проханням перейти за посиланням для «проходження перевірки», саме посилання нагадує адресу сайту, та насправді не веде на офіційний онлан-ресурс. За посиланням пропонується лише додати новий пристрій до вашого акаунта, після чого зловмисник отримує доступ до всієї історії переписок та може вести їх від імені жертви. [18]

Частими є випадки телефонного шахрайства з отриманням SMS-повідомлення чи дзвінка про банківські операції, які насправді не здійснювались. Таким чином зловмисники направляють жертв до банкомату і просять виконати певні дії – для перевірки. Та все вище зазначене робиться з метою викрадення коштів.

4. Watering hole – почуття: приналежність.

Метод полягає у розміщенні злоякісного програмного забезпечення на сайтах, які часто використовує організація, людина та подальше їх зараження з метою отримання доступу до захищеної системи. [5] Такими сайтами можуть бути: сайти компаній-партнерів, соціальних організацій та урядових установ, [8] куди жертви заходять на постійній основі або досить часто, що пов'язано зі сферою їх діяльності, належністю до певних груп, чи просто звичкою щодо перегляду новин.

Однією зі схем роботи шахраїв є повідомлення від Служби безпеки України своїм співробітникам про необхідність у зазначені терміни, з наголосом на «терміново», ознайомитись з електронним планом евакуації та надати данні про чисельність персоналу заповнивши форму документу, перейшовши за вказаним посиланням та наступним отриманням конфіденційної інформації. [18]

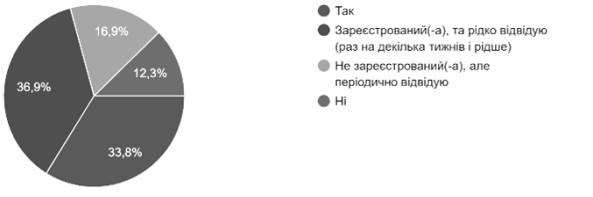
Іншим способом збору даних для входу в особистий кабінет одного з банків ніби-то від імені Червоного Хреста України був шахрайський чат-бот «Червоний Хрест Допомога» (redcrossuabot) – спроба доступу до захищеної системи. [17]

5. Бейтінг – почуття: зацікавленість.

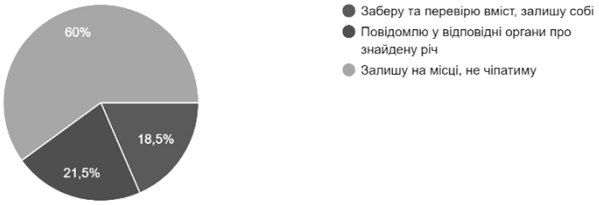
Метод, являє собою розвідувальну діяльність і полягає в організації підставних обставин, підкинутих предметів котрі привертають увагу, дій в мережі спеціального форуму, сайту куди запрошують людей певної групи інтересів [5].

Перерахована діяльність спрямована на пробудження інтересу та бажання скористатись запропонованою наживкою у результаті чого, зазвичай, відбувається зараження пристрою, контроль над мережею або отримання секретних даних.

Питання 7-8 розділу 2 визначали ймовірність впливу бейтінгу, і результатом є діаграми 7-8.



Діаграма 7. Розділ 2. Вплив соціальних інженерів на Вашу особистість. Питання 7. Чи є Ви зареєстрованим користувачем певних сайтів, груп, пабліків та відвідуєте їх на постійній основі (кожного дня, де-кілька раз на тиждень)?



Діаграма 8. Розділ 2. Вплив соціальних інженерів на Вашу особистість. Питання 8. Як Ви вчините зі знайденим носієм чи накопичувачем інформації (флешка, диск)?

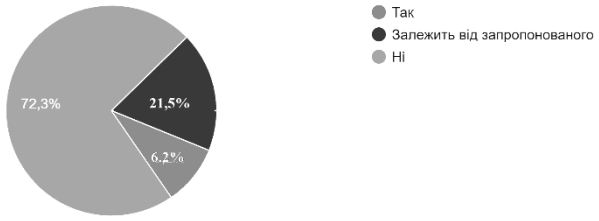
Відповіді на питання вказують на те, що близько 70% опитаних є користувачами різних груп, форумів, зібрань відповідно до сфер інтересів і доволі часто їх відвідують, а тому несвідомо можуть бути залучені до підставних шахрайських формувань, з метою ведення спостереження та вивчення користувача. Також 40%, що є доволі високим показником, готові забрати знайдену річ у власне використання, тим самим наражаючи себе та свій пристрій на злом, зараження, віддалений контроль.

Доволі часто диверсійні групи використовують даний метод для розповсюдження цінних речей, технічних гаджетів, котрі можливо і не несуть на меті зараження пристоїв, але можуть бути заміновані, що значно гірше, оскільки призводить до втрати життя. Окрім того, діяльність зазначених груп автоматично додають людей у чати з назвами «Перекличка районів» аби дізнаватись дані про міста та коригувати ворожий вогонь. [17]

6. Quid Pro Quo – почуття: довірливість.

Метод описує сутність виразу «щось за щось» - обмін. Користуючись даним методом зловмисник представляє себе працівником технічної підтримки, та пропонує виправити проблеми в системі, котрі насправді відсутні. [3] Жертва вірить в наявність несправностей, і виконуючи вказівки хакера власноруч встановлює шкідливе програмне забепечення типу шифрувальника даних [3].

Питання 9 розділу 2 визначало ймовірність впливу впливу методу Quid Pro Quo - діаграма 9.



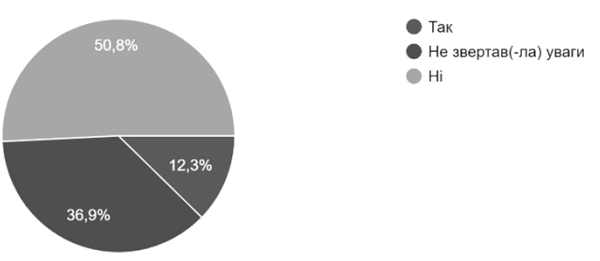
Діаграма 9. Розділ 2. Вплив соціальних інженерів на Вашу особистість. Питання 9. Чи повідомите Ви будь-які конфіденційні дані взамін на грошову винагороду чи значущу послугу?

Тож вигода, для деяких людей все ж має значення, саме про це свідчить результат у 21,5%, готових проміняти свою безпеку, ймовірно, на грошову винагороду, а 6,2% зроблять це навіть не задумуючись. І з точки зору інформаційної безпеки тут доцільно розглянути принцип Парє, лише з певною видозміною: 10-10-80. Це означає, що змоделювавши дану ситуацію у контексті бізнесу можна отримати наступний результпат: 10% співробітників компанії будуть шкодити завжди, ще 10% - ніколи не завдадуть проблем, а інші 80% - будуть діяти відповідно до обставин. І більша частина цих 80% все ж здійснять певне правопорушення. Що і доводить ефективність застосування методу Quid Pro Quo.

7. Переслідування – почуття: неуважність.

Метод використовується для отримання доступу в захищену зону. Спостерігач очікує доки авторизований користувач відкриє та пройде через захищений прохід, а потому слідує за ним. [5]

Питання 10 розділу 2 дозволяє визначити певний відсоток використання методу переслідування - діаграма 10.



Діаграма 10. Розділ 2. Вплив соціальних інженерів на Вашу особистість. Питання 10. Чи спостерігали Ви, що за Вами стежать чи фотографують невідомі особи?

Стає очевидним, що більша частина, у майже 60% живуть безтурботним життям, не звертаючи уваги на навколишнє середовище, та все ж деякі особи є цікавими – 36,9%.

8. Зворотня соціальна інженерія – почуття: довірливість, неуважність.

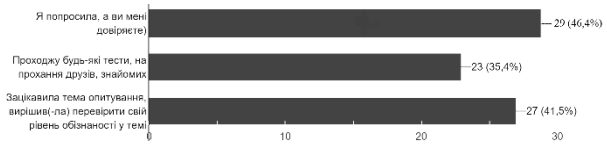
Метод спрямований на провокування жертви самій звернутись до соціального інженера та надати йому конфіденційні дані. [3] Це досягається шляхами впровадження особливого програмного забезпечення та рекламою. Стосовно першого сценарію, провокується збій системи, що потребує втручання спеціаліста, котрим виступає соціальний інженер, до якого звертаються по допомогу. Налагоджуючи роботу, шахрай проводить необхідні для злому маніпуляції. При викритті злому, зловмисник не буде під підозрою, оскільки «допомагав». Другий спосіб подається рекламою послуг комп'ютерного майстра, звертаючись до якого, потерпілий надає зловмиснику технічний доступ та можливість отримання інформації через особисте спілкування, викликаючи почуття довіри через допомогу. [3]

Питання 11 дало змогу оцінити ймовірність впливу зворотньої соцальної інженерії на опитуваних. Як результат – діаграма 11.

Як виявляється, 7,7% хоча б раз потрапляли на шахраїв, що виявлялись чудовими маніпуляторами та ошукували своїх «клієнтів».

Діаграма 11. Розділ 2. Вплив соціальних інженерів на Вашу особистість. Питання 11. Чи бували Ви жертвою "комп'ютерних майстрів", котрі під приводом допомоги та налагодження вашого пристрою отримували конфіденційну інформацію про Вас, та шантажували?

Отже, важливо відзначити, що навіть, беручи до уваги третій закон Ньютона про силу дії, котрій завжди рівна силі протидії, як у випадках: є віруси – наявні антивіруси, є вторгнення хакерів ззовні, як і протидія вторгненням – IPS/IDS системи і т.д., що на будь-який шкідливий вплив на інформаційно-технологічну систему буде знайдена контрміра. Та виключення – соціальна інженерія. Проводивши дане опитування мною було розіслано запрошення на його проходження у вигляді посилання на Google-форму з проханням допомогти. І от що вийшло у результаті – діаграма 12.



Діаграма 12. Розділ 4. Питання 1. Ви перейшли для проходження опитування за цим посиланням, тому що...

За наявної можливості обрати кілька варіантів відповідей найбільший відсоток отримав варіант мого прохання, та довіри до мене – 46,4%. І не менш цікавим є те, що лише декілька людей з опитуваних попередньо поцікавились що це тест та з якою метою проводиться, інша частина не намагалась переконатись у мене особисто, що: я це дійсно та людина котра видала себе за мене та чи мій обліковий запис не було скомпрометовано; дане для проходження опитування посилання не несе шкідливого змісту та не спрямовує на заражений сайт; знаючи мене як особу не може виникнути думки про протиправні дії з мого боку. Також привабливим є результат у 35,4%, який опитувані обрали зазначивши про байдужіть що проходити, якщо про це просять знайомі люди. Зацікавленість – третій варіант відповіді, також зіграла б проти самих опитуваних, як варіант застосування бейтінгу зі сторони шахраїв. Відтак, важливо акцентувати увагу на тому, що вищеперераховані та обрані відповіді дають змогу зробити висновок про можливість та актуальність здійснення

впливу соціальних інженерів описаними у розділі методами навіть на такому простому прикладі, як дружнє прохання по послугу.

Тож соціальна інженерія - це те, проти чого не існує прийому, оскільки атакують людину. І відносно до стрибкоподібного росту технологій, мозок людини не еволюціонував настільки швидко та не опанував навичок виявлення і протидії соціальній інженерії, окрім наявності критичного мислення та параноїдального відчуття.

Соціальна інженерія на основі технологій що розвиваються (біологічний фактор).

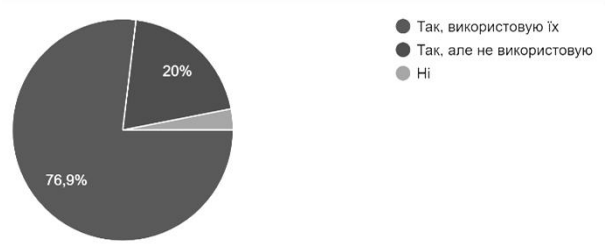
Кожна з розглянутих надалі технологій може бути застосована у якості розширення до вже існуючих методів соціальної інженерії, так як полегшує вплив на свідомість з урахуванням улюблених ефектів зловмисників: поспіху, несподіванки, спантеличення, викликання почуття жалю, тривоги, бурхливої радості.

Відтак, розділ 3 опитувальника містить питання спрямовані на визначення обізнаності та розуміння рівня розвитку та застосованості сучасних інформаційних технологій у повсякденному житті – діаграми 13-15.

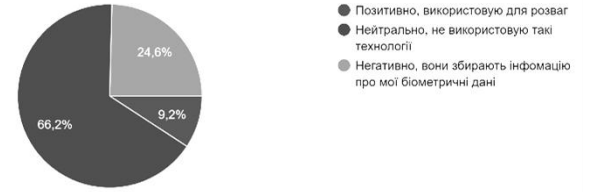
Результатом опрацювання даних є те, що майже всі 100% ознайомленні з вищевказаними методами та засобами біометричної автентифікації, та 76,9% є активними користувачами зазначених технологій. Такий результат свідчить про широке розповсюдження та щоденне використання біометричних даних у якості паролів та ідентифікаторів користувачів електронних пристроїв і встановлених сучасних технологій.

Розглядаючи діаграму 14 стає помітно що переважна кількість опитаних не зважають на розвиток додатків, що використовують підміну почерку, голосу, лиця. Але частка у 24,6% все ж з певною обережністю відносяться до таких технологій. Та чи не вважають вони часом ймовірним використання даних технологій для підробки фінансових документів, перерахунку коштів, компрометації осіб? І як видно 80% дійсно можуть задумуватись над цим, та всерйоз стурбованими залишається лише половина.

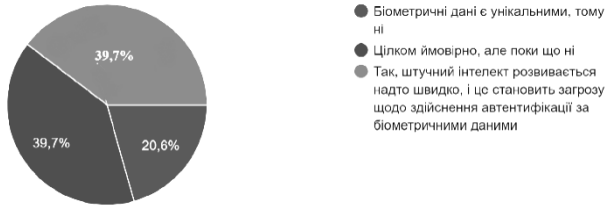
Тож, спираючись на отримані результати, при описі наступних технологій розглядається потенціал використання останніх з методами соціальної інженерії.



Діаграма 13. Розділ 3. Ставлення до розвитку сучасних інформаційних технологій. Питання 1. Чи знаєте Ви про методи та засоби біометричної автентифікації (відбиток пальця, FaceID і т.д.)?



Діаграма 14. Розділ 3. Ставлення до розвитку сучасних інформаційних технологій. Питання 2. Як Ви ставитеся до технологій та додатків, що використовують підміну почерку, голосу, лиця?



Діаграма 15. Розділ 3. Ставлення до розвитку сучасних інформаційних технологій. Питання 3. Чи вважаєте Ви ймовірним використання даних технологій для підробки фінансових документів, перерахунку коштів, компрометації осіб?

1. Підробка почерку.

Розроблений алгоритм «My Text in your Handwriting» [9] призначений для відображення бажаного рядка рукопису авторським почерком. Здійснення копіювання рукопису є доволі складним завданням, оскільки природний почерк дуже мінливий, але разом з тим містить певні структурні закономірності, що відображає певний стиль. [9] Тож і зазначений алгоритм використовує підхід із вивченням параметрів інтервалу, товщини лінії та тиску і створює нові зображення рукописного вводу. Для навчання алгоритму достатньо одного абзацу рукопису, після, будь-який текст може бути написаний вашим почерком.[9] На сьогодні, це найточніша реплікація. На даний момент програма не є повністю автоматичною, завдяки складності розпізнавання окремих букв і елементів, а також особливостей аналогових записів (ручка яка не дописала букву, десь натисли сильніше, десь розмазалось) - але за допомогою нейронних мереж це вирішиться досить швидко. [10] Наразі, такий метод не пройде графологічну експертизу (там багато перевірок, в тому числі і фізичних параметрів нанесення тексту на папір), але це теж справа недалекого майбутнього. [10]

Для зловмисників дана технологія на перспективу створює високий потенціал обману - від підробки фінансових документів до зміни історії.

2. Підміна голосу.

Канадський стартап Lyberid анонсував сервіс Descript's Ovrlab [12], який можна використати для підробки голосу будь-якої людини. Для навчання системи достатньо хвилини запису оригіналу. За цей час вона «генерує унікальний ключ», за допомогою якого може опрацювати будь-яку вимову, надаючи їй характеристик необхідного голосу. [11] В якості демонстрації технології розробники згенерували ключі для голосів Дональда Трампа, Барака Обами та Хілорі Клінтон. Приклади, опубліковані на сайті, досить показові [11]. Wave Net Google [12] та Resemble.AI [13] надають аналогічний функціонал, але ще не довершені та потребують більше нових навчальних фрагментів.

Завдяки цим технологіям все більшого розвитку та поширення набуває система голосового фішингу. Злочинці легко спрямують оперативні служби по помилковому шляху, будуть в змозі видати себе за іншу людину, з метою розіграшу, або ж для перерахунку коштів на чужий рахунок.

3. Штучний діалог.

Компанія Luka створила додаток Replika [15], який дозволяє створювати цифрову копію людини. Технологія навчається у свого власника та з його соцмереж, після чого в змозі виступати в його ролі: підтримувати бесіду, призначати зустрічі та проводити їх. [14]

Для соціальних інженерів, дана технологія - це чудова нагода здійснення шантажу, шляхом видання себе за впливових персон, керівників компаній.

4. Заміна лиця.

Популярна технологія Deep Fake, дозволяє замінювати обличчя на відеозаписі. Робота штучного інтелекту полягає в об'єднанні декількох фото із зображенням людини та створенні відео. Аналізуючи велику кількість зображень штучний інтелект навчається тому, як може виглядати та рухатись певна особа. [16] Складніші алгоритми можуть генерувати відео на яких людина робить і говорить те, чого ніколи не робила. [16] Технологія, ще не досягла максимальної правдоподібності, але вчені прогнозують підвищення якості заміни лиця та можливості робити це у реальному часі.

Тож для злочинців, це чергова нагода: вплив на різні аспекти життя людства, зіпсована або знищена репутація, політична дезінформація, корпоративний саботаж, залякування.

Висновки

Наукова новизна отриманих результатів дослідження свідчить про те, що вже зараз людство входить в епоху, де охорона кожного біту інформації про кожну особу є центральним питанням особистої безпеки, і не лише в цифровому світі. Залишається лише усвідомити та навчитись протидіяти можливим загрозам компрометації даних та подальших наслідків.

Як видно, з перерахованих методів соціальної інженерії вони всі працюють, оскільки виглядають правдиво та експлуатують довіру користувачів, спонукаючи останніх до дій. Тому варто зберігати скептицизм та пильність напротивагу неуважності і довірливості; не переходити на підозрілі сайти та завантажувати сумнівні файли, чому передує цікавість; не використовувати один пароль на всіх можливих платформах, що являє собою легковажність; не працювати з важливою інформацією на очах у сторонніх – пересторога; не поширювати персональну інформацію на відкритих сторінках соціальних мереж – темна сторона відкритості.

У статті подана мала частка технологій котрі розвиваються, набирають великих обертів та створюють все кращі умови для здійснення шахрайства соціальними інженерами: імітація голосу, почерку, лиця. І не виключено, що згодом, навчання штучного інтелекту може призвести до загроз стосовно проведення процедур автентифікації та авторизації користувачів за біометричними даними.

Перелік посилань

1. На грані фантастики: як шахраї стануть розорювати компанії в майбутньому. [Електроний ресурс] – Режим доступу: https://pro.rbc.ru/demo/6139acfc9a7947c551a0204e. – 13.12.2021 р.
2. Чому соціальна інженерія залишається головною зброєю кіберзлочинців. [Електроний ресурс] – Режим доступу: https://www.crn.ru/news/detail.php?ID=152522. – 13.12.2021 р.
3. Обережно, це пастка: що таке соціальна інженерія. [Електроний ресурс] – Режим доступу: https://www.reg.ru/blog/chto-takoe-sotsialnaya-inzheneriya/ – 12.12.2021 р.
4. Соціальна інженерія в епоху соціальної ізоляції. [Електроний ресурс] – Режим доступу: https://habr.com/ru/company/dsec/blog/556812/. – 14.12.2021 р.
5. Що таке соціальна інженерія? [Електроний ресурс] – Режим доступу: https://10guards.com/ru/articles/what-is-social-engineering/. – 13.12.2021 р.
6. Турбіна для SOC: як системи SOAR прискорюють реагування на кіберінциденти. [Електроний ресурс] – Режим доступу: https://www.securitylab.ru/analytics/527425.php. – 13.12.2021 р.
7. Що таке фішинг. [Електроний ресурс] – Режим доступу: https://interesnyefakty.org/chto-takoe-fishing/. – 13.12.2021 р.
8. Атаки типу watering hole стають улюбленою зброєю хакерів. [Електроний ресурс] – Режим доступу: https://tcinet.ru/press-centre/technology-news/460/. – 15.12.2021 р.
9. Том С.Ф. Хейнс, Ойсін Мак Аодха, Габріель Дж. Бростоу. Мій текст твоїм почерком. [Електроний ресурс] / Том С.Ф. Хейнс, Ойсін Мак Аодха, Габріель Дж. Бростоу. – Режим доступу: http://visual.cs.ucl.ac.uk/pubs/handwriting/. – 14.12.2021 р.
10. Програма копіює почерк. [Електроний ресурс] – Режим доступу: https://pikabu.ru/story/programm_kopiruet_pocherk_skaynet_pobedit_na_samom_dele_net_4806136?view=amp. – 14.12.2021 р.
11. Створена перша технологія для підробки будь-яких голосів. [Електроний ресурс] – Режим доступу: https://habr.com/ru/post/403413/. – 14.12.2021 р.
12. Надреалістичне клонування голосу за допомогою Overdub. [Електроний ресурс] – Режим доступу:https://www.descript.com/overdub?lyrebird=true. – 15.12.2021 р.
13. Стандартні та WaveNet голоси. [Електроний ресурс] – Режим доступу: https://cloud.google.com/text-to-speech/docs/wavenet#standard_voices. – 13.12.2021 р.
14. Фролов. А. Російський стартап Luka анонсував сервіс для створення цифрової копії людини Replika. [Електроний ресурс] / Фролов А. – Режим доступу: https://vc.ru/flood/18530-luka-replika. – 14.12.2021 р.
15. Replica. [Електроний ресурс] – Режим доступу: https://replika.ai/. – 14.12.2021 р.
16. Чи будемо почуватися безпечно в інтернеті в 2020 році. [Електроний ресурс] – Режим доступу: https://trends.rbc.ru/trends/industry/5e1c655a9a794756aa4f03d6. – 14.12.2021 р.
17.Телеграм-канал Державної служби спеціального зв'язку та захисту інформації України. [Електроний ресурс] – Режим доступу: https://t.me/dsszzi_official. – 19.05.2022р.
18. Офіційний канал Служби безпеки України. [Електроний ресурс] – Режим доступу: https://t.me/SBUkr. – 21.05.2022р.

Надійшла: 21.01.2022 Рецензент: д.т.н., професор Савченко В.А.