КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4(16), 2022
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2022.15.4562
УДК 004.056

Лаптєв Сергій Олександрович
Аспірант кафедри кібербезпеки та захисту інформації
Факультет інформаційних технологій
Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID ID: 0000-0002-7291-1829
salaptiev@gmail.com

УДОСКОНАЛЕНИЙ МЕТОД ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ВІД АТАК ЗА ДОПОМОГОЮ АЛГОРІТМІВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Анотація. Соціальна взаємодія суб'єктів у сучасному світі крім позитивних форм має і негативні. У сучасному суспільстві неможливо обійтися без соціальних мереж і в сучасному світі переважають інтернет - технології. В даний час кожна людина, пов'язана з комп'ютером, зареєстрована хоча б в одній соціальній мережі. Соціальні мережі притягують людей, так як в сучасному світі всі люди спілкуються, обмінюються інформацією, знайомляться, частина людей придумує для себе віртуальний світ, в якому вони можуть бути безстрашними, популярними за допомогою чого відмовляються від реальності. Проблема, пов'язана з безпекою персональних даних в соціальних мережах є найбільш актуальною і цікавою в сучасному соціумі.

Аналіз методів захисту персональних даних від атак за допомогою алгоритмів соціальної інженерії, показав що неможливо віддати перевагу якомусь одному методу захисту персональної інформації. Усі методи захисту персональних даних цілеспрямовано впливають на захист інформації, але захист в повному обсязі неможливо забезпечити тільки одним методом.

Спираючись на аналіз методів захисту персональних даних, нами запропоновано удосконалений метод захисту персональних даних від атак за допомогою алгоритмів соціальної інженерії. Удосконалення полягає у поєднання двох вже існуючих методу які спрямовані на підвищення ефективності навчання користувачів. Використовуючи сформульовані нами особливості запропонованого методу, саме підвищення навчання користувачів забезпечить більш якісний захист персональних даних.

В якості головної переваги запропонованого методу є теє що використовується синергія існуючих методів, які цілеспрямовані на навчання користувачів, навчання захисту своїй особистої персональної інформації.

Напрямок подальшого дослідження: аналіз та удосконалення методів атак не тільки за допомогою фішінгової соціальної інженерії а також за допомогою інших методів соціальної інженерії інших типів. Створення математичної моделі захисту персональної інформації від атак за допомогою методів соціальної інженерії.

Ключові слова: метод, соціальна інженерія, персональні дані, атака, захист інформації.

ВСТУП

Соціальна інженерія – це такий нетехнічний тип стратегії кібератак, який базується на взаємодії між людьми та маніпуляціях таким чином, щоб людина порушила стандартні правила кібербезпеки. Для таких атак не потрібно бути хакером і знати купу технічної інформації, тому зловмисники активно використовують дану тактику. Легше обманом отримати бажане, ніж зламувати програмне забезпечення, наприклад, людина за власним бажанням передає вам свій пароль, аніж ви спробуєте зламати його. Проте соціальна інженерія вимагає від зловмисника гарної підготовки, що зазвичай має на меті збір інформації про жертву, аби точно знати, як саме можна отримати бажану інформацію.

Закон України “Про інформацію” [1] окреслює конфіденційну інформацію як інформацію про фізичну особу, а також інформацію, доступ до якої обмежено фізичною або юридичною особою. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом. У сучасному світі найуразливішою ланкою серед усіх кібератак залишається людина. Персональні дані можуть бути як конфіденційною інформацією, так і відкритою. Пункт 2 статті 11 Закону України “Про інформацію” [1] встановлює, що конфіденційними є зокрема дані про національність, освіту, сімейний стан, релігійні переконання, стан здоров’я, місце проживання і/або реєстрації, дата і місце народження. Закон України “Про захист персональних даних” [2] визначає персональні дані як відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Це найуживаніше визначення даного поняття - і воно є найбільш узагальненим. Перелік відомостей, які належать до персональних даних, змінюється від однієї держави до іншої. Наприклад, інформація про IP-адресу в країнах Європейського Союзу належить до персональних даних, а у Сполучених Штатах Америки ні, проте відноситься до інформації, що пов’язана з персональними даними.

Сучасні підприємства створюють кіберзахист, орієнтуючись насамперед на технічні вектори атак. Такі системи можуть мати високий рівень зрілості і здаватися надійними, але при цьому залишатися уразливими для однієї з найнебезпечніших загроз - соціальної інженерії, заснованої на маніпуляціях людською свідомістю. За статистикою, сьогодні соцінженерія так чи інакше застосовується в 97% націлених атак, при цьому технічні вектори часом взагалі не використовуються або використовуються мінімально. На перші місця серед загроз інформаційної безпеки ставляться методи соціальної інженерії, а ряд вчених стверджує, що якщо соціальна інженерія візьме на озброєння технології машинного навчання і штучного інтелекту, то людство отримає загрозу, яку можна порівняти з глобальним потеплінням і ядерною зброєю. У просунутих варіантах соціальна інженерія - це витончена галузева політика «професійних» команд шахраїв і технічних фахівців різних профілів.

Тому питання вивчення методів впливу на безпеку персональної інформації – соціальної інженерії є дуже актуальним.

Постановка проблеми. Основне протиріччя, яке лежить в основі наукового дослідження полягає, в тому, що персональна інформація, яка передається та зберігається, не завжди може бути представлена у вигляді даних чи відомостей на машинних носіях у стандартизованому чи формалізованому вигляді, а, від так потребує особливих підходів щодо її захисту від спотворення.

Тому, зважаючи на комплексний характер загроз безпеці конфіденційним даним в умовах глобалізації та вільного обігу інформації в інформаційній сфері, вирішенню підлягає актуальне наукове завдання щодо розроблення методів та засобів виявлення несанкціонованого розповсюдження інформації в умовах інформаційного протиборства для захисту інформаційних ресурсів підприємств та установ.

Аналіз останніх досліджень і публікацій. Згідно з українським законодавством не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини. А отже, загрози персональним даним можна описати наступним чином - це загрози несанкціонованого зберігання, використання та поширення конфіденційних даних.

У статті [3] розглядається соціальна інженерія як метод нападу на персональні дані. Ситуація ускладняється тім, що користувачі самі не контролюють розповсюдження персональних даних. Це суб’єктивний фактор, якій спорила витоку персональних даних. Для забезпечення нормального функціонування, прийняття адекватних рішень

завданням кінцевого користувача є одержання об'єктивної своєчасної інформації про веб додатки, для чого на передній план виступають питання оцінювання достовірності веб додатків. Але методи захисту персональної інформації не розглядаються.

У статтях [4,5,6] обговорюється загрози безпеки персональних даних. Загалом, під атакою на персональні данні за допомогою соціальної інженерії розуміється потенційно можлива подія, процес або явище, яке за допомогою впливу на інформацію може прямо або опосередковано призвести до порушення конфіденційності, цілісності або доступності цієї інформації, а також має можливість впливу на компоненти інформаційно-комунікаційних систем, що призводить до їх втрати, знищення або збою функціонування, тим самим наносячи шкоду інтересам суб'єктів інформаційних відносин. Але закони несанкціонованого розповсюдження інформації не набули розкриття у цих джерелах.

У статтях [7-9] обговорюється суть та аналіз атак за допомогою соціальної інженерії. Цифрові данні це та суть, яку не можна поторкати, а значить на неї не поширюються деякі, звичні нам правила і закони. Аналіз можна визначити як діяльність по вивченню персональних даних, висновки по стану справ зараз, побудові прогнозів на основі цих даних і виробленню рекомендацій. Але аналіз обмежується лише осмислюванням отриманих даних та атак на них. Яка можлива шкода або можлива користь; як використати нові можливості або запобігти негативу у статтях не розглядається.

У статтях [10-12,14] надано акцент на те, що аналізом захищеності персональних даних ми займаємося постійно. Кожні нові потреби у персональної інформації викликає деякі процеси, які дозволяють нам оцінити отриману інформацію, зіставити з наявною, зробити які то виведення і т.п. наведені основні питання інформаційного аналізу. Але шляхи та алгоритми аналізу та оцінки персональної інформації не наводяться.

Разом з тим, незважаючи на значну кількість публікацій щодо вирішення захисту від різноманітних аспектів атак на персональні дані в умовах цифрового суспільства на сьогоднішній день залишається невирішеною проблема комплексного захисту персональних даних з урахуванням атак за допомогою методів соціальної інженерії.

Тому вивчення атак на персональні дані за допомогою методів соціальної інженерії в умовах інформатизації суспільства є актуальним знаковим завданням.

Мета статті. Проаналізувати існуючи методи соціальної інженерії. На основі проведеного аналізу удосконалити метод захисту персональних даних від атак соціальної інженерії шляхом розробки тренінгу з вирішення проблеми реальними випадками.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Загрози персональним даним можна описати наступним чином - це загрози несанкціонованого зберігання, використання та поширення конфіденційних даних.

За згодою суб'єкта персональних даних конфіденційна інформація може оброблятися і зберігатися розпорядником, мету в цей час визначає володілець даних. Таким чином, володілець і розпорядник несуть відповідальність за дотримання конфіденційності довіреної їм інформації. Будь-які дані зберігаються в інформаційних системах, а отже, мова про загрози персональним даним, які зберігаються та обробляються в ІС (інформаційних системах).

Усі загрози можна умовно поділити на такі, які можуть бути реалізовані внаслідок атак, та такі, які не залежать від атак.

Загрози, які не пов'язані з цілеспрямованими атаками, можуть як призвести до втрати, спотворення або компрометації персональних даних суб'єкта, так і створити умови для їх використання зловмисниками.

ISSN 2663 - 4023

Такими загрозами можуть бути:

- такі, що не пов'язані з діяльністю людини: стихійні лиха та природні явища (землетруси, повені, урагани тощо);
- загрози соціально-політичного характеру: страйки, диверсії, локальні конфлікти, війна, що супроводжуються нападом на об'єкт, що містить ресурси інформаційної системи, тощо;
- помилкові дії та/або порушення персоналом та користувачами інформаційної системи вимог до відповідної експлуатаційної, організаційної, технічної чи іншої документації;
- загрози антропогенного характеру, наприклад: аварії та різного роду несправності та перешкоди, що призводять до порушень і збоїв у роботі апаратних компонентів інформаційної системи.

Закон України “Про інформацію” [1] окреслює конфіденційну інформацію як інформацію про фізичну особу, а також інформацію, доступ до якої обмежено фізичною або юридичною особою. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом

Захист від загроз, які не залежать від атак, регулюється інструкціями, розробленими та затвердженими уповноваженими службами розпорядника персональних даних, з урахуванням специфічних умов функціонування інформаційної системи, а також чинних нормативних документів.

Захист від загроз, які можуть бути реалізовані внаслідок атаки, повинен забезпечуватися за допомогою захисних заходів і засобів, які використовуються інформаційною системою і призначені переважно для протидії атакам.

Атака соціальної інженерії має спільну структуру. Вони відбуваються в один або кілька кроків [15].

На рис. 1 схематично зображений життєвий цикл атаки.

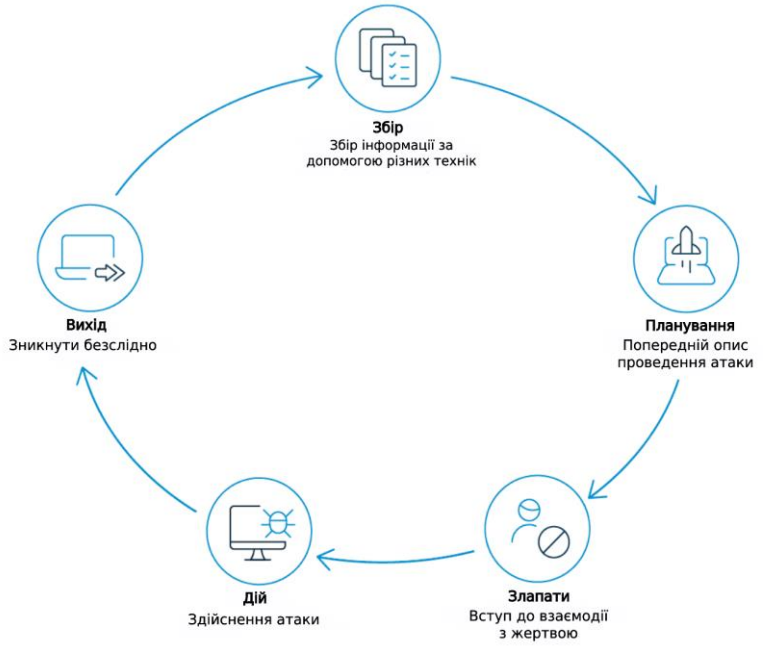

Рис. 1 Життєвий цикл атаки.

Згідно цій схеми, існують наступні етапи підготовки та здійснення атаки:

ISSN 2663 - 4023

1. Збір інформації та планування. Імовірність успіху більшості атак залежить саме від цієї фази, тому є логічним, що зловмисники приділяють цьому етапу більшу частину свого часу та уваги. Інформація може збиратися різними методами. Маючи правильну інформацію, зловмисник може визначити вектор атаки, можливі паролі, ймовірні відповіді окремих осіб й уточнити цілі. На цьому етапі зловмисник дуже добре ознайомлюється з жертвою та формулює конкретний план атаки під дану особу.

2. Встановлення контакту з жертвою та взаємодія. На цьому етапі зловмисник встановлює контакт з жертвою та вибудовує довірливі стосунки. Це критична точка, оскільки якість встановленого контакту визначає рівень співпраці та міру, з якою жертва буде допомагати зловмисникові досягти мети. Наприклад, це може бути доволі короткотривалий контакт, як поспішати до дверей з широкою посмішкою та зоровим контактом, щоб жертва притримала двері відкритими для зловмисника. Це може бути особисте спілкування по телефону або смол-ток з секретарем у фойє. Водночас цей етап може бути більш масштабним - таким, як побудова онлайн-знайомство та встановлення стосунків із жертвою за допомогою фальшивого профілю на сайті знайомств або в соціальних мережах.

Після цього зловмисник використовує як зібрану інформацію, так і встановлений контакт, не викликаючи підозр. Далі відбувається взаємодія зловмисника і жертви, наприклад, це може бути реалізовано шляхом розголошення, здавалося б, неважливої інформації або доступу, наданого/переданого зловмиснику. Приклади успішної фази взаємодії включають:

- утримання дверей відкритими або введення зловмисника всередину приміщення;
- розкриття пароля та імені користувача по телефону;
- вставлення флеш-накопичувача USB із шкідливим ПЗ до комп’ютера компанії;
- відкриття зараженого вкладення електронної пошти
- розкриття комерційної таємниці під час обговорення з нібито «знайомим».

3. Виконання атаки. Ця фаза — це коли зловмисник досягає своєї кінцевої мети. Як правило, атака закінчується ще до того, як жертва починає розуміти, що відбувається. Натомість зловмисник має на меті закінчити атаку таким чином, щоб жертва почувалася так, ніби вона зробив щось корисне для “знайомого”, тим самим забезпечуючи можливу подальшу взаємодію.

4. Вихід з атаки. Зловмисник стирає цифрові відбитки будь-якого свого перебування. В результаті нападник досягає двох важливих цілей. По-перше, жертва не знає, що напад відбувся. По-друге, зловмисник приховує свою особу. Добре спланована і плавна стратегія виходу є метою нападника і останнім актом в атаці.

Сфера застосування соціальної інженерії достатньо широка, однак визначають основні напрямки, сфери:

- збір відкритої інформації про жертву, а саме з’ясування інтересів та особливостей поведінки потенційної жертви, соцмереж, якими вона користується, а також імен, під якими вона з’являється у мережі Інтернет, через ведення діалогу з нею або з її оточенням у службах обміну миттєвими повідомленнями;
- отримання конфіденційної інформації про об’єкт атаки або інформації, що становить для зловмисника певний інтерес, наприклад номери телефонів потенційної жертви, адресу її реєстрації, проживання, реальне ім’я та прізвище тощо, через встановлення контакту з нею або шляхом оману;
- отримання інформації про об’єкт атаки, необхідної для забезпечення несанкціонованого доступу до системи, а саме пароля, яким користується потенційна жертва, серії та номеру паспорта та інших відомостей про неї шляхом входження в довіру до обраної жертви;

- примушення жертви до дій, необхідних порушникові, через нав'язування такому об'єкту нової моделі поведінки. Наприклад. Проникнення в мережу організації для дестабілізації з певною метою роботи її основних вузлів;
- загальна дестабілізація роботи в організації з метою зниження її впливу, а згодом і повного її знищення;
- фінансові махінації в організації;
- фішинг та інші способи викрадення паролів із метою доступу до персональних даних тощо;
- викрадення клієнтських баз. Інформація про маркетингові плани організації. Загальна інформація про організацію, її сильні і слабкі ланки з метою подальшого знищення. Часто застосовується для рейдерських атак. Інформація про найбільш перспективних співробітників із метою їх подальшого переманювання до своєї організації.

Атаки соціальної інженерії не втрачають своєї популярності, з часом з'являються нові типи маніпулювання людьми, а отже і типи атак. На рис.2. зображені основні типи атак соціальної інженерії.

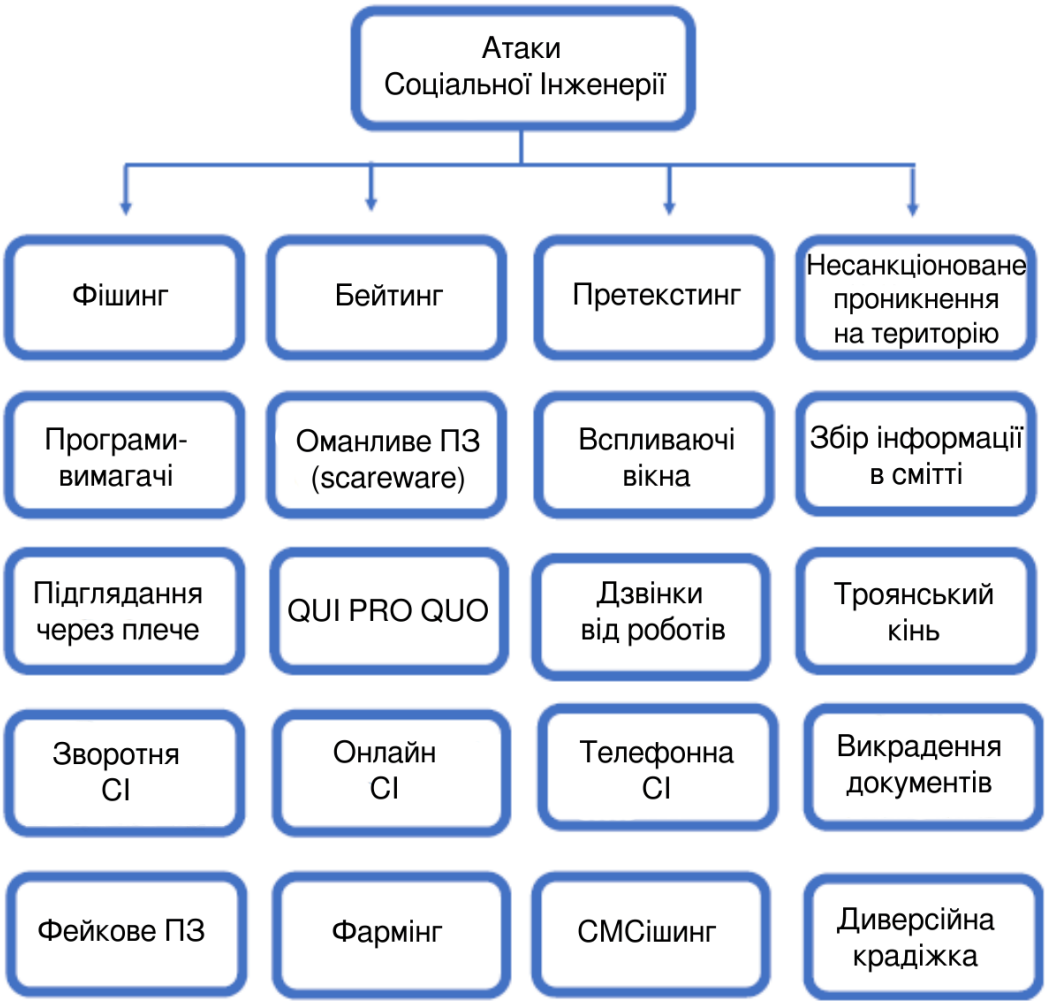

Рис. 2 Основні види атак соціальної інженерії

Основне припущення які ми вводимо у роботі, це те що основним видом атаки на персональні дані будемо враховувати фішинг атаку.

ISSN 2663 - 4023

Фішинг — це такий тип атак, за якого зловмисник обманним шляхом заволодіває конфіденційною інформацією. В основному зловмисники використовують даний тип атак використовуючи електронну пошту. Відтак існують найпопулярніші сценарії. Коли зловмисник надсилає фішинговий лист, він має на меті – змусити користувача виконати певні дії, щоб отримати певні дані для подальшої атаки, або ж встановити шкідливе програмне забезпечення як частину більш широкомасштабної спроби проникнення. Фішингова атака матиме більше шансів бути успішною, якщо атака персоналізована під конкретного користувач. Таким чином зловмисник створює ілюзію того, що електронний лист отриманого з надійного джерела, а отже, це підвищує ймовірність того, що користувач прочитає цей лист або навіть виконає дії згідно з рекомендаціями зловмисника. Усі фішинг атаки можуть бути поділені на 5 груп (рис 3): спрямований фішинг, полювання на корпоративних китів, телефонний фішинг, інтерактивний фішинг голосової відповіді та компромісний фішинг для ділової електронної пошти.

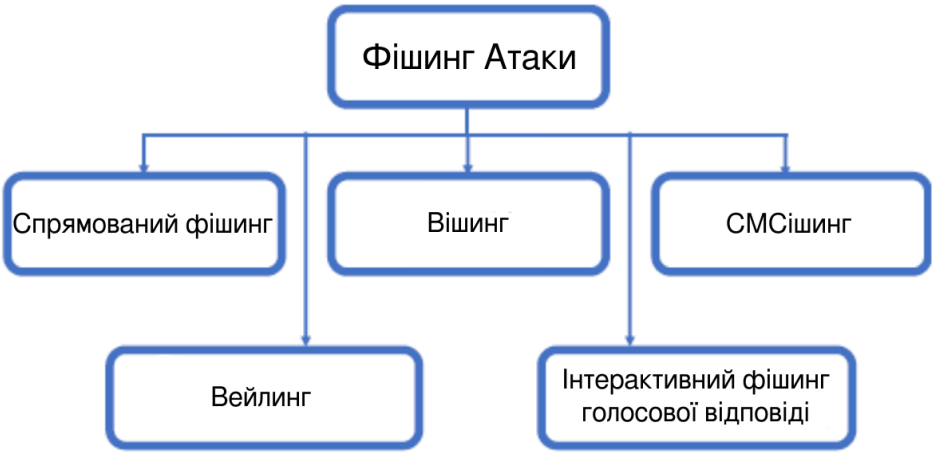

Рис. 3. Основні різновиди фішинг атак.

Спрямований фішинг (Spear phishing) – це цілеспрямована фішингова атака. Як звичайний, так і спрямований фішинг використовують електронну пошту, щоб досягнути мети. Але у випадку спрямованого фішингу персоналізовані електронні листи надсилають конкретній особі. Перед відправленням такого електронного листа зловмисник вивчає інтереси потенційної жертви. Найчастіше жертвами спрямованого фішингу є високі посадові особи, які мають доступ до більшої конфіденційної інформації, аніж пересічний робітник.

Вішинг(англ. Vishing від поєднання Voice та Fishing) або телефонний голосовий фішинг або – це такий тип атаки, коли кіберзлочинець дзвонить за номером телефону й за допомогою створення відчуття невідкладності ситуації змушує людину вчиняти проти своїх інтересів. Такі дзвінки зазвичай відбуваються в стресовий час, наприклад, посеред ночі, коли людина раптово прокидається і має зрозуміти, що відбувається. Ці атаки є популярними, оскільки телефонні дзвінки знеособлені, оскільки жертва не бачить співрозмовника. А це надає неабиякі переваги зловмиснику, оскільки завжди можна покласти слухавку і, наприклад, викинути сім-карту. У більшості країн вже існує обов'язкова реєстрація номеру з прив'язкою до паспортних даних особи, але навіть за такого сценарію, користувач має на це певний проміжок часу до блокування сім-карти, а це дає можливість бути знеособленим деякий період.

СМС фішинг (Smishing) – це вид фішингу, який використовує текстові повідомлення на мобільних телефонах. Злочинці видають себе за офіційне джерело, щоб завоювати довіру жертви. Наприклад, під час СМС фішингу зловмисник може надіслати

жертві посилання на веб-сайт. Коли жертва відвідає цей веб-сайт, на мобільний телефон буде встановлене зловмисне ПЗ. Також популярний сценарій смс-фішингу, це смс-повідомлення з довільного або прихованого номеру ніби-то від банку з текстом «Vasha karta bude zablokovana bankom. Terminovo proidit avtorizaciu, abo zatelefonuite…».

Вейлінг (*Whaling* полювання на корпоративних китів) – це фішингова атака, що спрямована на осіб, які мають повний доступ до інформації у межах організації, наприклад, її вище керівництво. Також цілями можуть бути політики або знаменитості. Термін вейлінг походить від розміру атак, а китів вибирають відповідно до їхніх повноважень у компанії. Через чітко спрямований характер вейлінг-атаки часто важче виявити, ніж стандартні фішинг-атаки. На підприємстві адміністратори безпеки можуть допомогти знизити ефективність вейлінг-атак, залучаючи співробітників корпоративного управління пройти навчання з інформаційної безпеки.

Інтерактивний фішинг голосової відповіді виконується за допомогою інтерактивної системи голосового реагування, щоб жертва вводила приватну інформацію так, ніби вона отримала дзвінок від знайомого бізнесу або банку.

Виявлення фішингових атак

Можливо виокремити два основних підходи до виявлення фішингу: навчання користувачів і за допомогою програмних засобів [16].

1) *Навчання користувачів*: користувачів можна навчити краще розуміти природу фішингових атак, що в результаті допоможе коректно розрізняти фішингові і справжні повідомлення. Це суперечить категоризації в роботі [17], де навчання користувачів розглядається як превентивний захід. Однак навчання має на меті розпізнавання користувачами фішингових атак, тому розглядається як підхід до виявлення фішингу.

2) *За допомогою програмних засобів*: цей підхід має на меті заповнити прогалину, яка виникає через помилку користувача або незнання, та розрізняти програмним способом фішингові та легітимні повідомлення. Цей недолік вимагає вирішення, оскільки навчання користувачів є дорожчим, ніж автоматична класифікація, та не завжди є можливим, наприклад, коли бази користувачів є завеликими (PayPal, eBay, Amazon тощо).

Розпізнавання фішингової атаки – це початкова точка протидії фішинговим атакам. На рис. 4 показана схема підходів до розпізнавання фішингових атак.

Рис. 4 Схема алгоритму розпізнавання фішингових атак

Ефективність виявлення може бути покращена за рахунок навчання класифікатора (як людини, так і ПЗ). У випадку з навчанням користувачів якість виявлення може бути покращена за рахунок їхнього індивідуального досвіду або за допомогою зовнішніх навчальних програм. У випадку програмної класифікації ефективність може бути підвищена в процесі в процесі "навчання" класифікатора, побудованого на алгоритмах машинного навчання, або вдосконаленням правил виявлення в системі на основі правил.

Програмний підхід до виявлення

Чорні списки. Це постійно оновлюванні списки, що містять раніше виявлені фішингові URL-адреси. Недоліком даної методології є затримка в оновленні списків. Для того, щоб щойно створений фішинговий сайт потрапив у список, необхідний час. Цієї затримки між відправленням даних і додаванням сайту до списку може бути достатньо для досягнення зловмисниками своїх цілей.

Білі списки. Ці списки є чимось протилежним до чорних. Якщо є певна URL-адреса, її порівнюють з легітимною адресою зі базою даних "білого списку". База даних «білого списку» здебільшого містить список популярних справжніх URL-адрес та їхні важливі дані. Як і у випадку з чорним списком, для завантаження нової відомої URL-адреси може знадобитися певний час, через який. зловмисник, безсумнівно, може досягти своїх цілей.

Евристичні методи виділяють певні характеристики веб-сторінки для того, щоб визначити легітимність веб-сайту, а не залежати від будь-яких попередньо скомпільованих списків. Це перевага евристичних методів, над "списками". Більшість цих характеристик витягуються з URL-адреси та дерево об'єктної моделі документа HTML (DOM) даної веб-сторінки. Вилучені характеристики порівнюються з вже відомими, що були зібрані з фішингових та справжніх сторінок, щоб визначити їх легітимність. Деякі з цих підходів використовують евристики для обчислення оцінки підробки даної веб-сторінки, щоб перевірити її справжність. [18,19]

Сучасні веб-браузери та поштові клієнти побудовані з механізмами захисту від фішингу, такими як евристичні тести з метою виявлення фішингових атак. Так само евристичні тести виявлення фішингу можуть бути включені в антивіруси.

Методи візуальної схожості. Це методи розрізнення фішингових сайтів та легітимних сайтів за зовнішнім виглядом сайтів. Зазвичай фішингові сайти є майже точними копіями справжніх, щоб у користувача не виникали сумніви щодо легітимності ресурсу. З метою не бути виявленими зловмисники, як правило, вставляють зображення, Flash, ActiveX і Java-аплет замість HTML-тексту. Методи виявлення на основі візуальної схожості можуть швидко розпізнавати перераховані об'єкти на веб-сторінках фішингових сайтів. Методи, засновані на візуальній схожості, використовують підпис, щоб розрізняти фішингові сторінки. Щоб зробити підпис потрібно вибирати спільні компоненти з усього сайту, а не з окремої сторінки веб-сайту. Таким чином, одного підпису достатньо, щоб ідентифікувати різні цільові веб-сторінки окремого веб-сайту або унікальні форми веб-сайту. Даний метод використовує для порівняння дерево об'єктної моделі документа HTML (DOM), схожість каскадної таблиці стилів (CSS), візуальне сприйняття, візуальні особливості, піксельні та гібридні підходи [22-23].

Машинне навчання [12] забезпечує спрощені та ефективні методи аналізу даних, останнім часом демонструючи багатообіцяючі результати у проблемах класифікації в реальному часі. Ключовою перевагою машинного навчання є можливість створювати гнучкі моделі для конкретних завдань, таких як виявлення фішингу. Оскільки фішинг є проблемою класифікації, моделі машинного навчання можна використовувати як потужний інструмент. Моделі машинного навчання можуть швидко адаптуватися до

змін, щоб визначити моделі шахрайських операцій, які допомагають розробити систему ідентифікації на основі навчання.

На рис. 4 наведені два підходи до виявлення фішингових атак: навчання користувачів та програмний підхід. Для цієї роботи було обрано більш детально розглядати підхід навчання користувачів.

Незалежно від наявних навичок чи здібностей, усі люди в організації мають пройти навчання з антифішингу. Для боротьби з фішингом існує багато методів до навчання користувачів. На рисунку 3.2 зображені деякі з основних [17].

Лекції. Це один з найстаріших методів і він досі лишається одним із найпоширеніших, незважаючи на свої недоліки. Залучення користувачів до лекцій обмежується слуханням, конспектуванням, синтезом та упорядкуванням знань. Даний метод не вимагає будь-якого обладнання, окрім як наявність лектора та охоплення великої кількості матеріалу на одну лекцію. Матеріал також має бути логічним та структурованим для усного сприйняття, що полегшує навчання персоналу без додаткових друкованих або онлайн матеріалів.

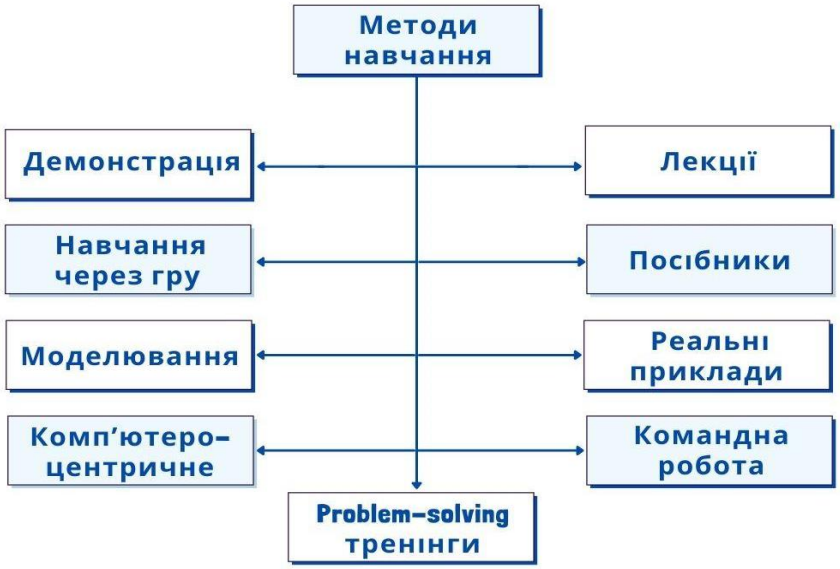

Рис. 5 Методи навчання користувачів

Попри те, що цей метод досі користується популярністю для навчання користувачів, він має недоліки, зокрема наступні:

- для лекцій потрібні ефектні доповідачі;
- потрібен інтерактив і гарна взаємодія лектора з аудиторією, інакше користувачі, як правило, швидко втрачають концентрацію та інтерес;
- від співробітників очікується, що вони навчатимуться в однаковому темпі та з однаковим розумінням, а це не так;
- виявленню фішингових атак у реальному часі не можна навчити лише на лекціях, для успіху потрібно залучати інші ресурси.

Навчальні посібники, гайди та мануали. У навчанні користувачів навчальний посібник є необхідним для поглиблення знань з теми. За допомогою посібників вони можуть дізнатися, як можна практикувати вдома або у вільний час. Існує багато різновидів навчальних посібників, наприклад:

- робочі зошити зазвичай використовуються на навчальних курсах, де конспектуються основні поняття, схеми та приклади фішингу;
- інструкції для самостійної роботи, які учні можуть виконувати у вільний час;

- довідкові посібники часто використовуються, щоб дізнатися більше про процеси та процедури;
- роздатковий матеріал містить загальну інформацію, яка доповнює матеріал, який викладає тренер на сесії.

Водночас одним із недоліків посібників є те, що користувачі можуть не зрозуміти деякі важливі поняття, просто читаючи матеріал.

Навчання на реальних прикладах. Це ретельне дослідження конкретного випадку або ситуації в реальному часі. Такий метод має можливість зробити процес навчання набагато більш реалістичним. Метою вивчення конкретного випадку є краще зрозуміти проблему. Таким чином, тренери надають детальні описи ситуації, дають можливі пояснення та оцінюють вирішення проблеми. Цей метод може використовувати різноманітні прийоми для збору інформації, включаючи інтерв'ю, спостереження, експерименти, опитувальники тощо. У контексті фішингу проводиться велика кількість тематичних досліджень, щоб оцінити труднощі та можливі рішення.

Групове навчання. Користувачі можуть поглибити свої знання під час командної роботи. Спільне навчання може допомогти слухачам покращити свою продуктивність. Очікується, що команди отримають нові навички та інформацію, а також допоможуть іншим членам опанувати нові навички та інформацію. Наприклад, різні антифішингові команди в кіберпросторі співпрацюють, щоб знайти відповідні рішення для боротьби з фішингом. Недоліком цього методу навчання є те, що всі залежать один від одного.

Тренінг із вирішення проблем – це тип навчання, під час якого людина вчиться знаходити найкраще ефективне рішення проблеми, наприклад, фішингу. Навчання з вирішення проблем полягає в тому, щоб користувачі проходили три кроки. Визначення різних типів фішингових атак є першим кроком до їх подолання. Для цього користувачі повинні зібрати інформацію про фішингові атаки. Наступним кроком є висування слухачами ідеї щодо боротьби з фішинг-атакою. Після цього слухачі мають проголосувати або оцінити рішення для зменшення можливості фішингової атаки. На останньому етапі від слухачів вимагається втілити рішення, яке було обрано на попередньому етапі.

Демонстрація. Демонстрації, як правило, включають покрокове навчання. Наприклад, дуже важливо, щоб учні збирали фішингові дані в реальному часі та практикували те, чому їх навчили тренери. Багато експертів проводять живі демонстрації того, як зловмисник створює та здійснює фішингову атаку. Демонстрація може бути невдалою, якщо тренери не планують її належним чином. Це вимагає великої підготовки.

Навчання через гру. Існує кілька способів практикувати фішинг, але один з найпоширеніших – це гра. Навчання через гру є більш приємним, покращує засвоєння інформації та стимулює запам'ятати більше і краще. Таким чином, фішингові атаки краще розуміються через гру. Наприклад, гравці повинні ідентифікувати фішингові веб-сайти, надані тренером, щоб отримати бали.

Навчання на основі моделювання є високоефективним і економічно вигідним методом навчання слухачів у реальному часі в контрольованому середовищі. Це дає тренерам найкращий шанс побачити, наскільки добре слухачі реалізують свої таланти на практиці та приймають рішення щодо виявлення фішингу в імітованих реальних обставинах. Слухачі натомість отримують чудовий практичний досвід. Недоліком цієї стратегії є те, що зловмисники модифікують набору інструментів, що робить користувачів вразливими до атак.

Комп'ютерне навчання – це такий метод навчання, який покладається на використання цифрових технологій, таких як ноутбуки та планшети, щоб замінити традиційне навчання в класі. Зазвичай це робиться онлайн за допомогою системи управління навчанням (LMS) і може бути виконано з будь-якої точки світу. У комп'ютерному навчанні використовується багато основних методів, і одним з них є

онлайн-вікторина. Вміння користуватися комп'ютером є ключовим моментом цього навчання.

Проведений аналіз дозволяє зробити висновки про те, що кожен з описаних методів має певні недоліки. Тому з метою удосконалення методу захисту персональних даних від атак за допомогою алгоритмів соціальної інженерії, пропонується поєднати два з вже існуючих методів з метою підвищення ефективності навчання користувачів. Пропонується поєднати наступні методи: навчання на реальних прикладах, та тренінг із вирішення проблем. В результаті матимемо тренінг із вирішення проблем, що базується на реальних прикладах.

Суть даного тренінгу заключається в тому, аби пройти вікторину, що базується на реальних прикладах, які можуть зустрітися пересічному українцю. Суть розробленого тренінгу заключається в тому, аби пройти опитування, що базується на реальних прикладах, які можуть зустрітися пересічному українцю. Приклади змодельовані відповідно до реальних випадків. Приклади засновані на оголошенні з продажу мобільного телефону на онлайн-платформі оголошень OLX.

Не зважаючи на те, що вже навіть сама платформа випустила гайд [18] про те, як не віддати свої кошти зловмиснику, люди досі стають жертвами кіберзловмисників, а отже, приклад є актуальним.

Схема тренінгу. Знайомство і загальні питання. Приклад 1. Висновки з прикладу 1. Приклад 2. Висновки з прикладу 2.

Знайомство включає наступні питання.

1. Стать
2. Вік
3. Чи знаєте ви що таке фішинг?
4. Чи стикалися ви з фішингом?
5. Чи були ви ціллю зловмисника?
6. Чи здатні ви відрізнити фішингове повідомлення?
7. Чи вивчали ви раніше тему фішингу?

Вхідні дані для прикладу 1 і 2. Ви - продавець на онлайн-платформі оголошень OLX. Ви виставили на продаж певний дороговартісний товар, наприклад, мобільний телефон вартістю 10 000 грн. Вам дуже хочеться продати свій товар і отримати кошти.

Приклад 1. Слухачеві пропонується ознайомитися з повідомленнями (рис. 6).

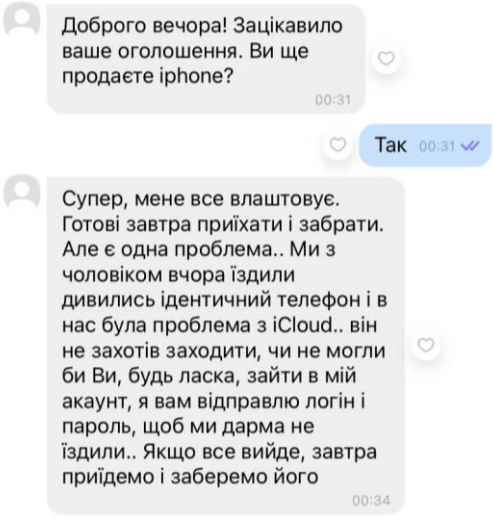

Рис. 6 Змодельовані повідомлення з прикладу 1

Далі слухач має зробити висновки і відповісти на питання.

1. Допоможете людині чи ні? І чому?
2. Як ви думаєте, яке буде продовження в цієї історії, якщо ви відповіли так і якщо ні?

Після цього наступним кроком слухачеві пояснюється даний приклад, суть та схема атаки та наводяться висновки.

Висновки з прикладу 1. Отже, приклад 1 - це типова схема вимагання грошей. По-перше, зловмисники використовують сторонній майданчик. Продавцеві з покупцем цілком можна обійтися платформою OLX для уточнюючих запитань. По-друге, зловмисники втираються до вас в довіру "щоб ми дарма не їздили.. " - таким чином намагаючись нав'язати вам відчуття провини, тобто чинять тиск на те, аби ви погодились. За успішного сценарію даної атаки - ви вводите в свій iPhone авторизаційні дані зовсім незнайомої вам особи. Відписуєте в месенджері "все ок, все вийшло". Далі ви, органічно, хочете вийти з акаунту цієї особи, але не можете. Оскільки пароль невірний. Компанія Apple вимагає підтвердження виходу з iCloud за допомогою пароля. Таким чином зловмисник має контроль над вашим телефоном. Зазвичай за новий пароль зловмисники просять викуп в розмірі 50% вартості телефону. Звісно, ви можете писати скарги в Apple, доводити їм, що телефон і справді ваш, а це велика прикрість, але цей шлях обере меншість. Більшість просто заплатить гроші, аби їм розблокували їхній же пристрій. Будьте обізнані та не ловіться!

Якщо ви знаєте про такого типу атаки, ви молодець! Якщо ви засумнівалися і почали шукати в інтернеті інформацію щодо такого типу атак, ви молодець! Що ви можете зробити, аби таких ситуацій траплялося менше? Поділитися із знайомими. Таким чином більше людей будуть готові та не повірять шахраю.

Що робити, якщо вас таким чином таки вдалося спіймати на гачок і ви відправили гроші? Написати заяву в кіберполіцію, оскільки вимагач надсилатиме вам номер картки, також ви матимете його номер телефону.

Приклад 2. Слухачеві пропонується ознайомитися з наступними повідомленнями (рис. 7).

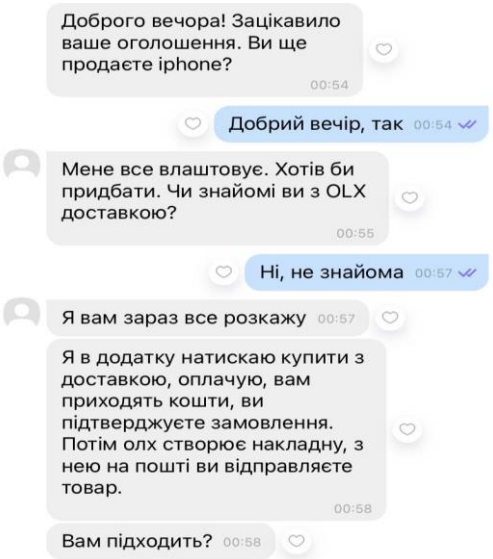

Рис. 7 - Змодельовані повідомлення для прикладу 2.

Далі слухач має зробити висновки і відповісти на питання.

1. Погоджуєтесь? Чому так або ні?
2. Як ви думаєте, яке буде продовження в цієї історії, якщо ви відповіли так і ні?

У випадку, якщо користувач погоджується, змодельований подальший розвиток

ISSN 2663 - 4023

подій. Пропонується наступний діалог до ознайомлення, та запитання, спрямовані на те, чи здатний слухач визначити фішингове посилання.

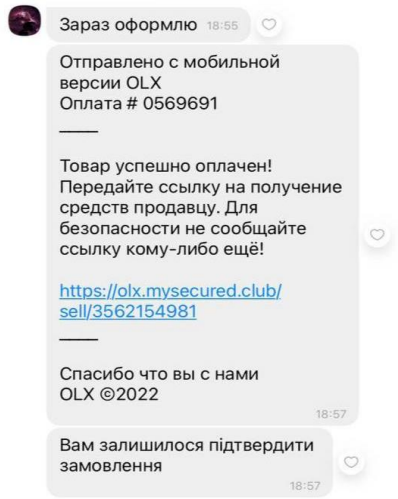

Рис. 8 Змодельовані повідомлення для прикладу 2.

Сучасні веб-браузери вже здатні вирізняти фішингові посилання (рис. 9), та можуть показувати попередження, коли користувач хоче перейти за зазначеним посиланням.

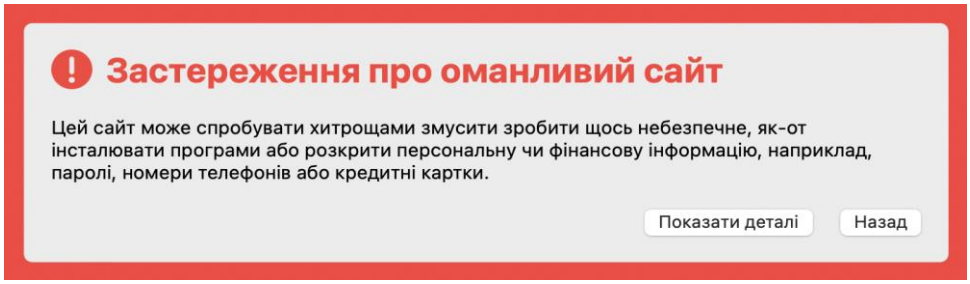

Рис. 9 Попередження про перехід на фішингову сторінку

Однак це відбувається не завжди. У випадку, якщо посилання відкривається, користувач побачить форму оплати (рис. 10), яка візуально майже ідентична до легітимного сайту.

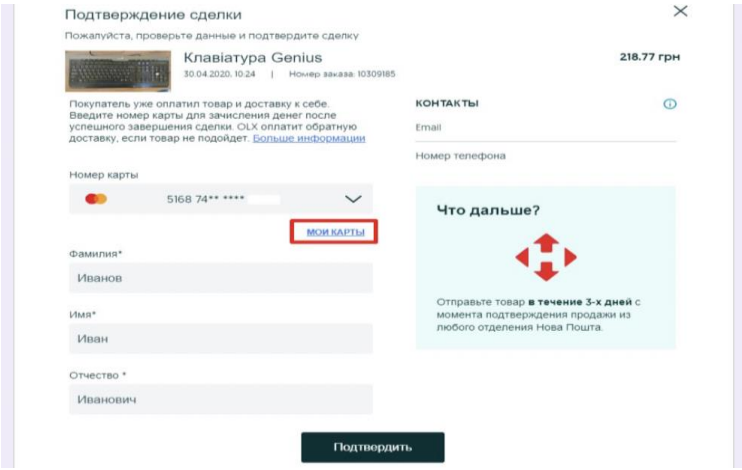

Рис. 10 - Фішингова форма оплати.

Після цього наступним кроком слухачеві пояснюється даний приклад, суть та схема атаки та наводяться висновки.

Висновки з прикладу 2. Не переходьте за посиланнями, які вам відправляють в особистих повідомленнях. Запам'ятайте це правило. Пам'ятайте, що в роботі послуги OLX Доставка відсутні будь-які індивідуальні форми і посилання для здійснення угоди / отримання коштів по угоді. Всю актуальну інформацію щодо купівлі-продажу ви можете побачити лише у своєму профілі в додатку або на веб-сайті.

Якщо ви відмовилися від такої OLX-доставки ще на початку, ви молодець! Поділіться з друзями. Найперше такі зловмисники пишуть також на сторонній ресурс - найчастіше Viber. Також варто звернути увагу на те, що фішингові повідомлення часто пишуться іншою мовою. Тобто ви спілкуєтесь українською, домовляєтесь українською, повідомлення з посиланням приходить російською. Це відбувається, наприклад, тому що сервіс для генерації фішингових посилань працює тільки російською. Наступним "дзвіночком" є те, що у зловмисника майже завжди немає уточнюючих питань, вони не намагаються збити ціну. Також зловмисники часто кваплять жертв, щоб у тої не було часу аналізувати те, що відбувається, тому зазвичай їхні легенди містять щось дуже термінове. Гарною вудочкою тут також є те, як саме шахраї пояснюють принцип роботи сервісу OLX-доставка. Воно майже відповідає дійсності, окрім моменту про те, що продавець отримує кошти до відправки. Згідно з даним сервісом, продавець отримує кошти лиш після того, як покупець забрав свою посилку з пошти і йому все підійшло. До того моменту, кошти вже списано з покупця, але вони знаходяться на рахунках OLX, і у випадку, коли покупцеві щось не підходить, він може відправити товар назад продавцеві і отримати свої кошти назад, відповідно, теж тільки після отримання продавцем товару, що не підійшов.

Таким чином удосконалення методу захисту персональних даних від атак за допомогою алгоритмів соціальної інженерії, здійснюється шляхом поєднання двох вже існуючих методу які спрямовані на підвищення ефективності навчання користувачів. Пропонується поєднати навчання на реальних прикладах, та тренінг із вирішення проблем. В результаті матимемо тренінг із вирішення проблем, що базується на реальних прикладах.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Аналіз методів захисту персональних даних від атак за допомогою алгоритмів соціальної інженерії, показав що неможливо віддати перевагу якомусь одному методу захисту персональної інформації. Усі методи захисту персональних даних цілеспрямовано впливають на захист інформації, але захист в повному обсязі неможливо забезпечити тільки одним методом.

Спираючись на аналіз методів захисту персональних даних, нами запропоновано удосконалений метод захисту персональних даних від атак за допомогою алгоритмів соціальної інженерії. Удосконалення полягає у поєднання двох вже існуючих методу які спрямовані на підвищення ефективності навчання користувачів. Використовуючи сформульовані нами особливості запропонованого методу, саме підвищення навчання користувачів забезпечить більш якісний захист персональних даних.

В якості головної переваги запропонованого методу є те що використовується синергія існуючих методів, які цілеспрямовані на навчання користувачів, навчання захисту своїй особистої персональної інформації.

Напрямок подальшого дослідження: аналіз та удосконалення методів атак не тільки за допомогою фішінгової соціальної інженерії а також за допомогою інших методів соціальної інженерії інших типів. Створення математичної моделі захисту персональної інформації від атак за допомогою методів соціальної інженерії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Закон України "Про інформацію". https://zakon.rada.gov.ua/laws/show/2657-12#Text.
2 Закон України "Про захист персональних даних". https://zakon.rada.gov.ua/laws/show/2297-17#Text
3 Бурячок, В. Л., Толубко, В. Б., Хорошко, В. О., Толюпа, С. В. (2015). Інформаційна та кібербезпека: соціотехнічний аспект : підручник. ДУТ.
4 Anti-Phishing Phil. https://www.cmu.edu/iso/aware/phil/index.html.
5 Фішинг в OLX Доставка. https://help.olx.ua/hc/uk/articles/360014371320-Фішинг-в-OLX-Доставка.
6 Хорошко, В. О., Хохлачова, Ю. Є. (2016). Information war. Mass media as an instrument of information influence on society. Part 1. *Ukrainian Scientific Journal of Information Security*, *22*(3). https://doi.org/10.18372/2225-5036.22.11104
7 Yoshihara, T. (2001). *Chinese information warfare: A phantom menace or emerging threat?* Strategic Studies Institute, U.S. Army War College.
8 Любарський, С. (2013). Місце та роль мережевої розвідки в моделях інформаційного протиборства. *Збірник наукових праць ВІТІ НТУУ «КПІ»*, (1), 31–39.
9 Laptiev, O., Savchenko, V., Kotenko, A., Akhramovych, V., Samosyuk, V., Shuklin, G., Biehun, A. (2021). Method of Determining Trust and Protection of Personal Data in Social Networks. *International Journal of Communication Networks and Information Security (IJCNIS)*, 13(1), 15-21.
10 Лаптев, О.А., Собчук, В.В., Саланди, И.П., Сачук, Ю.В. (2019). Математична модель структури інформаційної сеті на основі нестаціонарної ієрархічної та стаціонарної гиперсети. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка ВІКНУ*, 64, 124 – 132.
11 Laptev, A., Sobchuk, V., Barabash, O., Musienko, A. (2019). Analysis of the main Approaches and Stages for Providing the Properties of the Functional Stability of the Information Systems of the Enterprise .*Sciences of Europe*, *1*(42), 41 – 44.
12 Стефурак, О.Р., Тихонов, Ю.О., Лаптєв, О.А., Зозуля, С.А. (2020). Удосконалення стохастичної моделі з метою визначення загроз пошкодження або несанкціонованого витоку інформації. *Сучасний захист інформації: науково-технічний журнал*, *2(*42), 19 – 26.
13 Yevseiev, S., Laptiev, O., Korol, O., Pohasii, S., Milevskyi, S., Khmelevsky, R. (2021). Analysis of information security threat assessment of the objects of information activity. *International independent scientific journal*, *1*(34), 33 – 39.
14 10 популярных «фишинговых» тем в 2021 году по версии Positive Technologies. https://www.ptsecurity.com/ru-ru/research/analytics/10-populyarnyh-fishingovyh-tem-v-2021-godu-po-versii-positive-technologies/
15 Черняк, А. М., Прозоров, А. Ю. (2019). Аспекти запобігання правопорушенням у сфері використання банківських платіжних карток під час проведення безконтактних й інтернет-платежів та їх кваліфікація. *Naukovij visnik Nacional'noi akademii vnutrisnih sprav*, 4(113), 8-14.
16 Що таке фішинг? http://help.sslatcost.com/article/346?locale=uk.
17 *Фішинг (Phishing), Вішинг (vishing), Фармінг — шахрайство в Інтернеті Енциклопедія інтернет реклами*. (б. д.). Енциклопедія інтернет реклами. http://vse-prosto.весьтоп.рф/fishing-phishing-vishing-vishing-farming.html
18 Szafranski, R. *Theory of Information Warfare: Preparing For 2020*. Airpower Journal. http://www.airpower.au.af.mil/airchronicles/apj/apj95/spr95_files/szfran.htm

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (16), 2022
ISSN 2663 - 4023

Serhii Laptiev
PhD-student
Taras Shevchenko National University of Kyiv
Faculty of information tehnology
Department of Cyber Security and Information Protection
ORCID ID: 0000-0002-7291-1829
salaptiev@gmail.com

THE ADVANCED METHOD OF PROTECTION OF PERSONAL DATA FROM ATTACKS USING SOCIAL ENGINEERING ALGORITHMS

Abstract. Social interaction of subjects in the modern world, in addition to positive forms, also has negative ones. In modern society it is impossible to do without social networks and in the modern world the Internet - technologies prevail. Currently, everyone connected to a computer is registered in at least one social network. Social networks attract people, because in today's world all people communicate, exchange information, and get acquainted, some people come up with a virtual world in which they can be fearless, and popular and thus abandon reality. The problem related to the security of personal data in social networks is the most relevant and interesting in modern society.
Analysis of methods of protection of personal data from attacks using social engineering algorithms showed that it is impossible to prefer any one method of protection of personal information. All methods of personal data protection purposefully affect the protection of information, but protection in full can not be provided by only one method.
Based on the analysis of methods of personal data protection, we have proposed an improved method of protecting personal data from attacks using social engineering algorithms. Improvement is a combination of two existing methods aimed at improving the effectiveness of user training. Using the features of the proposed method formulated by us, it is the increase of user training that will provide better protection of personal data.
The main advantage of the proposed method is that it uses the synergy of existing methods, which are aimed at educating users and learning to protect their personal information.
The direction of further research: analysis and improvement of methods of attacks not only with the help of phishing social engineering but also with the help of other methods of social engineering of other types. Creating a mathematical model to protect personal information from attacks using social engineering methods.

Keywords: method, social engineering, personal data, attack, information protection.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1 Law of Ukraine "On Information". https://zakon.rada.gov.ua/laws/show/2657-12#Text ..
2 Law of Ukraine "On Personal Data Protection". https://zakon.rada.gov.ua/laws/show/2297-17#Text
3 Buriachok, V. L., Tolubko, V. B., Khoroshko, V. O., Toliupa, S. V. (2015). Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt : pidruchnyk. DUT.
4 Anti-Phishing Phil. https://www.cmu.edu/iso/aware/phil/index.html.
5 Fishynh v OLX Dostavka. https://help.olx.ua/hc/uk/articles/360014371320-Fishynh-v-OLX-Dostavka.
6 Khoroshko, V. O., Khokhlachova, Yu. Ye. (2016). Information war. Mass media as an instrument of information influence on society. Part 1. Ukrainian Scientific Journal of Information Security, 22(3). https://doi.org/10.18372/2225-5036.22.11104
7 Yoshihara, T. (2001). Chinese information warfare: A phantom menace or emerging threat? Strategic Studies Institute, U.S. Army War College.
8 Liubarskyi, S. (2013). Mistse ta rol merezhevoi rozvidky v modeliakh informatsiinoho protyborstva. Zbirnyk naukovykh prats VITI NTUU «KPI», (1), 31–39.
9 Laptiev, O., Savchenko, V., Kotenko, A., Akhramovych, V., Samosyuk, V., Shuklin, G., Biehun, A. (2021). Method of Determining Trust and Protection of Personal Data in Social Networks.

International Journal of Communication Networks and Information Security (IJCNIS), 13(1), 15-21.

10 Laptev, O.A., Sobchuk, V.V., Salandy, Y.P., Sachuk, Yu.V. (2019). Matematychna model struktury informatsiinoi seti na osnovi nestatsyonarnoi ierarkhichnoi ta statsionarnoi hypersety. Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka VIKNU, 64, 124 – 132.

11 Laptev, A., Sobchuk, V., Barabash, O., Musienko, A. (2019). Analysis of the main Approaches and Stages for Providing the Properties of the Functional Stability of the Information Systems of the Enterprise .Sciences of Europe, 1(42), 41 – 44.

12 Stefurak, O.R., Tykhonov, Yu.O., Laptiev, O.A., Zozulia, S.A. (2020). Udoskonalennia stokhastychnoi modeli z metoiu vyznachennia zahroz poshkodzhennia abo nesanktsionovanoho vytoku informatsii. Suchasnyi zakhyst informatsii: naukovo-tekhnichnyi zhurnal, 2(42), 19 – 26.

13 Yevseiev, S., Laptiev, O., Korol, O., Pohasii, S., Milevskyi, S., Khmelevsky, R. (2021). Analysis of information security threat assessment of the objects of information activity. International independent scientific journal, 1(34), 33 – 39.

14 10 populiarnыkh «fyshynhovыkh» tem v 2021 hodu po versyy Positive Technologies. https://www.ptsecurity.com/ru-ru/research/analytics/10-populyarnyh-fishingovyh-tem-v-2021-godu-po-versii-positive-technologies/

15 Cherniak, A. M., Prozorov, A. Yu. (2019). Aspekty zapobihannia pravoporushenniam u sferi vykorystannia bankivskykh platizhnykh kartok pid chas provedennia bezkontaktnykh y internet-platezhiv ta yikh kvalifikatsiia. Naukovij visnik Nacionalnoi akademii vnutrisnih sprav, 4(113), 8-14.

16 Shcho take fishynh? http://help.sslatcost.com/article/346?locale=uk.

17 Fishynh (Phishing), Vishynh (vishing), Farminh — shakhraistvo v Interneti Entsyklopediia internet reklamy. (b. d.). Entsyklopediia internet reklamy. http://vse-prosto.vestop.rf/fishing-phishing-vishing-vishing-farming.html

18 Szafranski, R. Theory of Information Warfare: Preparing For 2020. Airpower Journal. http://www.airpower.au.af.mil/airchronicles/apj/apj95/spr95_files/szfran.htm