Література:

1. Ukraine Data Explorer. URL: https://data.humdata.org/visualization/ukraine-humanitarian-operations/
2. Понад половина дітей України вимушено покинула свої домівки після місяця війни – ЮНІСЕФ. URL: https://www.unicef.org/ukraine/press-releases/more-half-ukraines-children-displaced-after-one-month-war
3. Як змінився освітній процес – на усіх його ланках – під час війни? URL: https://cutt.ly/AJaS5D7
4. 7 million children of war in Ukraine. URL: https://saveschools.in.ua
5. Куди запрошують українських науковців під час війни https://zn.ua/ukr/science/kudi-zaproshujut-ukrajinskikh-naukovtsiv-pid-chas-vijni.html
6. Вплив війни на середню освіту в Україні: виклики та перспективи https://cedos.org.ua/events/vplyv-vijny-na-osvitu-v-ukrayini-vyklyky-ta-perspektyvy/
7. Українська система вищої освіти в умовах воєнної агресії РФ: проблеми й перспективи розвитку. URL: https://niss.gov.ua/news/statti/ukrayinska-systema-vyshchoyi-osvity-v-umovakh-voyennoyi-ahresiyi-rf-problemy-y
8. The Future of Jobs Report 2020. URL: https://www.weforum.org/reports/the-future-of-jobs-report-2020/in-full/infographics-e4e69e4de7

DOI https://doi.org/10.36059/978-966-397-267-1/30

A METHOD OF PROTECTING SCIENTIFIC RESEARCH DATA FROM ATTACKS USING SOCIAL ENGINEERING ALGORITHMS

МЕТОД ЗАХИСТУ ДАНИХ НАУКОВИХ ДОСЛІДЖЕНЬ ВІД АТАК ЗА ДОПОМОГОЮ АЛГОРИТМІВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Sobchuk V. V.
Doctor Engineering, Associate Professor
Professor of the Department of Integral and Differential Equations
Faculty of Mechanics and Mathematics
Taras Shevchenko National University of Kyiv, Ukraine

Собчук В. В.
доктор технічних наук, доцент,
професор кафедри інтегральних та диференціальних рівнянь
механіко-математичний факультет
Київський національний університет імені Тараса Шевченка
Київ, Україна

Laptiev O. A.
Doctor of Technical Science, Senior Researcher
Associate Professor the Department of Cyber Security and Information Protection
Faculty of Information Technology
Taras Shevchenko National University of Kyiv, Ukraine

Лаптєв О. А.
доктор технічних наук,
старший науковий співробітник
доцент кафедри кібербезпеки та захисту інформації
факультет інформаційних технологій
Київський національний університет імені Тараса Шевченка
Київ, Україна

Sobchuk A. V.
Doctor of philosophy
Associate Professor of the Department of Information and Cyber Security,
State University of Telecommunications
Kyiv, Ukraine

Собчук А. В.
доктор філософії,
доцент кафедри інформаційної та кібернетичної безпеки,
Державний університет телекомунікацій
м. Київ, Україна

Laptiev S. O.
PhD-student
Taras Shevchenko National University of Kyiv
Faculty of information tehnology
Department of Cyber Security and Information Protection
Kyiv, Ukraine

Лаптєв С. О.
аспірант
факультет інформаційних технологій
кафедра кібербезпеки та захисту інформації
Київський національний університет імені Тараса Шевченка
Київ, Україна

Laptieva T. O.
PhD-student
Taras Shevchenko National University of Kyiv
Faculty of information tehnology
Department of Cyber Security and Information Protection
Kyiv, Ukraine

Лаптєва Т. О.
аспірантка
факультет інформаційних технологій
кафедра кібербезпеки та захисту інформації
Київський національний університет імені Тараса Шевченка
Київ, Україна

Найчастіше наукові установи 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 [1]. У соціальній інженерії [2] є кілька технік, використовуваних задля досягнення поставлених завдань. Усі вони засновані на помилках, які допускаються людиною у поведінці. Об'єктом впливу соціальної інженерії є не комп'ютерна техніка, а її користувачі. Інтерес представляють усі платоспроможні особи, а також користувачі, які мають цінну інформацію, співробітники підприємств та державних установ [3]. Метод застосовується для виконання фінансових операцій, злому, крадіжки відомостей (наприклад, клієнтських баз, персональних даних) та іншого несанкціонованого доступу до інформації. Соціальна

інженерія допомагає конкурентам здійснювати розвідку, виявляти слабкі сторони організації, переманювати працівників.

Зловмисники використовують соціальну інженерію для отримання матеріальної вигоди або видобутку даних для перепродажу. Соціальна інженерія може використовуватися як один з інструментів складних цільових кібератак. Джерелом загрози можуть бути електронні листи, текстові повідомлення у будь-яких месенджерах, SMS-повідомлення та телефонні дзвінки. Шахраї можуть видавати себе за співробітників банків та інших фінансових організацій, державних службовців, співробітників силових відомств, інтернет-провайдерів, представників поштових сервісів та великих веб-ресурсів тощо.

За статистикою, сьогодні соціальна інженерія 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 методи соціальної інженерії ставить і Gartner, 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.

Виклад основного матеріалу.

Сьогодні існує чимало методів використання соціальної інженерії. В основі – маніпуляція людськими страхами, зацікавленістю або довірою. Жертвою соціальної інженерії можна стати як під час особистого спілкування, так і по телефону або через цифрові гаджети [2].

Кіберзлочинці знайшли нові способи експлуатації людського фактору – інстинктів цікавості й довіри, – які призводять до того, що люди з добрими намірами потрапляють у руки зловмисників.

Популярні міфи, які стосуються соціальної інженерії:

1. Соціальна інженерія – обмежений набір технік. Прийнято вважати, що соціальна інженерія обмежується фішингом, підкиданням заражених флеш-накопичувачів, обманом в соціальних мережах і телефонним шахрайством. Насправді мова йде про практично нескінченної комбінації технічних і нетехнічних технік, що утворюють комплексні стратегії.

2. Соціальна інженерія – частина кібератак. Навпаки, кібератака може бути частиною загальної стратегії, основну частку якої займає соцінженерія.

3. Соціальна інженерія це в більшості випадків непередбачувана подія. Насправді соціальна інженерія завжди реалізується через таргетинг. У найпростіших випадках її фокус спрямований на організацію, в більш просунутих – на конкретну людину.

4. Соціальна інженерія можлива через низький рівень обізнаності у сфері інформаційної безпеки або низького рівня зрілості системи реагування на кіберінциденти та політики безпеки організації. Насправді соціальна інженерія за визначенням діє від розвіданого рівня обізнаності інформаційної безпеки та рівня зрілості системи ІБ, для чого завжди

починається з вивчення об'єкта атаки. Часто це найтриваліший і найбільш трудомісткий етап роботи соціального інженера.

Межі можливостей соціальної інженерії

У просунутих варіантах соціальна інженерія – це витончена галузева політика «професійних» команд шахраїв і технічних фахівців різних профілів. Щоб уявити, на що вони здатні, рекомендується вивчати не тільки відомі кібер інциденти, пов'язані з експлуатацією проблем людського фактора, а вивчити біографії найвидатніших соціальних інженерів (в т.ч. професійних шахраїв) за останнє сторіччя.

Як же працює соціальна інженерія? Кожна стратегія передбачає кілька етапів, і чим вище рівень зловмисника, тим менше він буде слідувати якимось певним скриптам послідовності дій [4]. Приклад життєвого циклу таких атак представлений на рисунку 1.

Рис. 1. Життєвий цикл соціальної інженерії

Кожен етап містить потенційно нескінченні комбінації нетехнічних заходів: техніки ініціації, первинної обробки, прийменників, добування інформації, впливу, обману і маніпуляції [5].

Окремо потрібно зупинитися на атаках на рівень підсвідомості. Це вкрай важливо для розуміння меж можливості захисту від витончених атак соціальної інженерії. Це більше теоретичне обґрунтування «на пальцях», але його досить для розуміння проблематики. Якщо розглядати соціальну інженерію як одну з ТОП-3 загроз людства, то в першу чергу тут йдеться про «злом» підсвідомості людського мозку, тобто коли дії атакуючих спрямовані не на рівень свідомості, а на рівень на підсвідомості.

Основні типи та види атак соціальної інженерії

Всі знають про зловмисника, який використовує свій технічний досвід для проникнення в захищені комп'ютерні системи і злому

конфіденційних даних. Цей тип зловмисників постійно робить новини, спонукаючи нас протистояти їх подвигам, інвестуючи в нові технології, які зміцнять нашу мережеву захист.

Однак є ще один тип зловмисників, які використовують різні тактики, щоб обійти наші інструменти і рішення. Їх називають «соціальними інженерами», тому що вони використовують одну слабкість, яка є в кожній організації: людська психологія. Використовуючи телефонні дзвінки та інші засоби спілкування з користувачами, ці зловмисники змушують людей передавати доступ до конфіденційної інформації організації.

У даній роботі буде розглянуто найбільш поширені типи атак, які використовують соціальні інженери:

Фішинг. Фішинг є найбільш поширеним типом атаки соціальної інженерії, яка відбувається сьогодні.

*Адресний фішинг.*У той час як більшість фішингових кампаній припускають масову розсилку електронних листів якомога більшій кількості користувачів, адресний фішинг відрізняється спрямованим характером. Цим способом зловмисники атакують конкретну особу або організацію, часто застосовуючи спеціально підібраний контент, який, як їм видається, надасть на жертву найбільший вплив

Клоновий фішинг. Цей тип атаки припускає, що зловмисники копіюють (клонують) раніше доставлене законне повідомлення, яке містить посилання або вкладення

*Обман 419 або нігерійські листи.*Багатослівне фішингових лист від невідомої особи, яка називає себе нігерійським принцом, є одним з найбільш ранніх і довгоживучих проявів подібних атак.

Телефоний фішинг. Фішингові атаки можуть відбуватися за допомогою звичайного телефону. В цьому випадку вони іноді позначаються як голосовий фішинг або «вішинг»

SMS-фішинг. SMS-фішинг (або «смішинг») – це злісний брат-близнюк вішинг, який здійснює ті ж шахрайські дії, але тільки за допомогою SMS-повідомлень (іноді додаючи до них шкідливі посилання).

Троянський кінь. Троянський кінь – це техніка ґрунтується на цікавості, страху або інших емоціях користувачів.

Послуга за послугу (Quid pro quo). Послуга за послугу – напади quid pro quo обіцяють вигоду в обмін на інформацію.

Привід. Привід – це ще одна форма соціальної інженерії, де зловмисники концентруються на створенні гарного приводу або сфабрикованої сценарію, який вони використовують, щоб спробувати вкрасти особисту інформацію своїх жертв.

Приманка (Bait). Приманка багато в чому схожа на фішингові атаки. Однак те, що відрізняє їх від інших видів соціальної інженерії – це обіцянка будь-якого предмета або блага, які зловмисники використовують для спокушання жертв.

Хвіст (Tailgating). У цих типах атак хтось без належної аутентифікації слід за перевіреним співробітником в обмежену область.

Дорожнє яблуко (Road apple). Дорожнє яблуко – цей метод є адаптацію троянського коня і полягає у використанні фізичних носіїв (CD, флеш-накопичувачів).

Зворотна соціальна інженерія. Зворотна соціальна інженерія – даний вид атаки спрямований на створення такої ситуації, при якій жертва змушена буде сама звернеться до зловмисника за «допомогою».

Приклади атаки соціальної інженерії в період військового стану.

Війна з росією вже зробила безпрецедентний вплив на різні сфери людської життєдіяльності, в тому числі на її сучасний технологічний уклад.

Кібератаки, які засновані на соціальної інженерії, часто співвідносяться з різними, вкрай хвилюючими ситуаціями. Події, пов'язані з війною не є винятком, особливо при нагнітанні обстановки. Сьогодні близько 88% актуальних новин в соцмережах присвячені війні. Негативні емоції новинної стрічки можуть бути обтяжені різного роду зловживаннями у використанні апарату математичної статистики. Об'єкти соціальних атак при війні мають принципову особливість. Для деяких співробітників компаній – це перший досвід віддаленої роботи. Не дивно, що за оцінками ряду фахівців, атаки соціальної інженерії, які спекулюють на тему війну як «приманки», домінують безпрецедентним чином. Наприклад, згідно з Cynet, з кінця лютого 2022 р число фішингових атак в Італії зросла аж в три рази! За заявою CheckPoint, за останні два тижні березня кількість зростання кібератак зросла в десять разів.

Слід відокремити, що існує декілька різновидів фішингових атак, а саме: атаки, які традиційно використовують інтернет-ресурси (пошту, веб-сторінки), текстові/SMS-повідомлення (ініціюють активну дію, шляхом обману) і голосові повідомлення (зокрема, використовують протокол VoIP).

Прикладами найпопулярніших типів атак соціальної інженерії, пов'язаних з війною є наступні:

1. Розсилка листів по електронній пошті з шкідливим вкладенням або посиланням на шкідливу програму або сайт. Джерела таких листів зазвичай маскуються під легітимні, наприклад, під керівника компанії, службу IT-підтримки, благодійну некомерційну організацію, фінансову або торговельну компанію (з дуже вигідними пропозиціями) та ін. Згідно з дослідженням TrenMicro, серед соціальних атак більше 65% становить саме спам-розсилка.

2. Пропозиції по установці шкідливих додатків, наприклад, карти поширення військових дій.

3. Відвідування фейковий веб-порталів, що маскуються під благодійні організації, страхові компанії. Фахівці з безпеки зафіксували вже вторинну хвилю появи обманних фішингових веб-сайтів, в назву яких входить похідні фрази віддаленого доступу – teams або zoom (додатки відео конференцій).

4. Фейкові новини, наприклад, що стосуються району знаходження, термінових повідомлень CDC, або просто вкидання, що паразитують на страху, стресі і нездоровому цікавості. Згідно з дослідженням британських вчених, при скоєнні комп'ютерних атак в 98% випадків використовуються методи соціальної інженерії. Зараз в Інтернеті представлено безліч яскравих прикладів тематичних атак, в тому числі українською мовою.

У стратегічному плані статистика сплеску кібератак в області соціальної інженерії і масове впровадження дистанційних робочих місць обумовлює необхідність і в удосконаленні нормативно-методичної бази захищеного віддаленого доступу, в першу чергу для інформаційних систем, які підлягають захисту відповідно до українського законодавства.

Висновки. Основним способом захисту від методів соціальної інженерії є розширення власних знань у сфері кіберзахисту, або навчання співробітників, якщо це стосується організації. Всі працівники компанії мають бути попереджені про небезпеку розкриття персональної інформації та конфіденційної інформації компанії, а також про способи запобігання витоку даних. Усі співробітники, в залежності від підрозділу і посади, повинен бути проінструктовані про те, як і на які теми можна спілкуватися зі співрозмовником, яку інформацію можна надавати для служби технічної підтримки, як і що повинен повідомити співробітник компанії для отримання тієї або іншої інформації від іншого співробітника.

Для захисту від атак на інформаційну безпеку підприємства за допомого соціальної інженерії необхідно проводити навчання у цьому напрямку. На підприємстві необхідно додати у свої навчальні програми по інформаційній безпеці, наступні пропозиції:

1. Не відкривайте електронні листи з ненадійних джерел. З кимось із друзів або членом сім'ї особисто або по телефону, якщо ви отримали від них підозріле повідомлення електронної пошти.

2. Не довіряйте пропозиціям незнайомих людей. Сумнівайтеся! Якщо пропозиції здаються занадто хорошими, щоб бути правдою, вони, ймовірно, це шахрайство.

3. Необхідно купити антивірусне програмне забезпечення. Жодне IT-рішення не може захистити від всіх загроз, які пов'язані з соціальною інженерією, але вони можуть допомогти захистити від деяких атак.

4. Призначені для користувача облікові дані є власністю компанії. Всім співробітникам в день прийому на роботу має бути роз'яснено те, що ті логіни і паролі, які їм видали, не можна використовувати в інших цілях (на web-сайтах, для особистої пошти тощо), передавати третім особам або іншим співробітникам компанії, які не мають на це право. Наприклад, дуже часто, йдучи у відпустку, співробітник може передати свої авторизовані дані свого колеги для того, щоб той зміг виконати деяку роботу або подивитися певні дані в момент його відсутності.

5. Необхідно проводити вступні та регулярні навчання співробітників компанії, спрямовані на підвищення знань з інформаційної безпеки. Проведення таких інструктажів дозволить співробітникам компанії мати актуальні дані про існуючі методи соціальної інженерії, а також не забувати основні правила по інформаційній безпеці.

6. Обов'язковою є наявність регламентів з безпеки, а також інструкцій, до яких користувач повинен завжди мати доступ. В інструкціях повинні бути описані дії співробітників при виникненні тієї чи іншої ситуації.

Наприклад, в регламенті можна прописати, що необхідно робити і куди звертатися при спробі третьої особи запросити конфіденційну інформацію або облікові дані співробітників. Такі дії дозволять обчислити зловмисника і не допустити просочування інформації.

7. У корпоративній мережі компанії необхідно використовувати системи виявлення та запобігання атак. Також необхідно використовувати системи запобігання витоку конфіденційної інформації.

8. Всі співробітники повинні бути проінструктовані, як вести себе з відвідувачами. Необхідні чіткі правила для встановлення особи відвідувача і його супроводу. Відвідувачів завжди повинен супроводжувати хтось із співробітників компанії. Якщо співробітник зустрічає невідомого йому відвідувача, він повинен в коректній формі поцікавитися, з якою метою відвідувач знаходиться в даному приміщенні і де його супровід. При необхідності співробітник повинен повідомити про невідомого відвідувача в службу безпеки.

9. Необхідно максимально обмежити права користувача в системі. Наприклад, можна обмежити доступ до web-сайтах і заборонити використання знімних носіїв. Адже, якщо співробітник не зможе потрапити на фішинговий сайт або використовувати на комп'ютері флеш-накопичувач з «троянською програмою», то і втратити особисті дані він також не зможе.

Основний спосіб захисту від соціальної інженерії – це навчання співробітників. Необхідно знати і пам'ятати, що незнання не звільняє від відповідальності. Кожен користувач системи повинен знати про небезпеку розкриття конфіденційної інформації і знати способи, які допоможуть запобігти витоку. Попереджений значить озброєний!

Література:

1. Пол Екман. Психологія брехні. Обдури мене, якщо зможеш. 2018, 2009, 2001, 1992, 1985 by Paul Ekman. 231c. 2018.

2. Кристофер Хєднгеги. Мистецтво обману: Соціальна інженерія в шахрайських схемах. 2018 by John Wiley & Sons, Inc., Indianapolis, Indiana. 2018. 235c. http://www.social-engineer.org.

3. Хенрік Фексеус. Мистецтво маніпуляції. Як не дати себе обдурити. Друкується з дозволу автора та літературних агенцій Grand Agency та Banke, Goumen & Smirnova Literary Agency, Sweden. 255 с. 2018

4. Serhii Laptiev. Удосконалений метод захисту персональних даних від атак за допомогою алгоритмів соціальної інженерії. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка & quot;, 4(16), 2022. С. 45–62. https://doi.org/10.28925/2663-4023.2022.16.4562 .

5. Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 188 p. 2021. DOI: 10.15587/978-617-7319-31-2

DOI https://doi.org/10.36059/978-966-397-267-1/31

PROBLEMATIC ISSUES OF TRAINING OF THIRD-LEVEL EDUCATION APPLICANTS IN UKRAINE

ПРОБЛЕМНІ ПИТАННЯ ПІДГОТОВКИ ЗДОБУВАЧІВ ТРЕТЬОГО РІВНЯ ОСВІТИ В УКРАЇНІ

Starinskyi M. V.
Doctor of Legal Sciences, Professor, Department of Administrative, Economic Law and Financial and Economic Security, Educational and Scientific Institute of Law Sumy State University, Sumy, Ukraine

Старинський М. В.
доктор юридичних наук, професор, професор кафедри адміністративного, господарського права та фінансово-економічної безпеки Навчально-наукового інституту права Сумського державного університету, гарант ОНП третього рівня 081 «Право» м. Суми, Україна

Сучасний розвиток вітчизняної системи освіти характеризується постійними змінами та трансформаціями. Починаючи з середини 2000-х років освітній процес постійно реформується, вдосконалюються і трансформуються існуючі інструменти реалізації освіти, виникають нові, що кардинально відрізняються від попередньо існуючих.

Починаючи з запровадженням в Україні Болонського процесу, ситуація з реформуванням у сфері освіти взагалі набула досить химерного характеру. Як свідчить аналіз змін, що відбулися під впливом вказаного процесу, вітчизняні реформатори для вдосконалення, взяли від Болонського процесу лише ту частину, яка була вигідна лише адмініструванню освіти, а не її якості. Як результат наступні роки пройшли в процесі підлаштування наявних механізмів вітчизняної освіти під «урізану Болонську систему». Наслідком цього в Україні сформувалась гібридна система вищої освіти з надзвичайно шкідливими для її якості механізмами, особливо в частині роботи науково-педагогічних працівників.

Також варто вказати, що в середині 2010-х років самі родоначальники Болонського процесу визнали його неефективним та