Живка Т.С.,
студент 6 курсу,4 групи, Інституту прокуратури та кримінальної юстиції Національного юридичного університету імені Ярослава Мудрого

СОЦІАЛЬНА ІНЖЕНЕРІЯ: СУЧАСНІ ВИКЛИКИ У ВІРТУАЛЬНОМУ ПРОСТОРІ

Ключові слова: кіберзлочинність, соціальна інженерія, хакери, інтернет-ресурс, фішинг, віртуальний простір.

Ключевое слово: киберпреступности, социальная инженерия, хакеры, интернет-ресурс, фишинг, виртуальное пространство.

Keyword: cybercrime, social engineering, hackers, Internet resource, phishing, cyberspace.

Анотація. В тезах здійснено аналіз такого виду кіберзлочинності як соціальна інженерія. Розглянуто основні способи її вчинення та заходи захисту від останньої.

Аннотация. В тезисах осуществлен анализ такого вида киберпреступности как социальная инженерия. Рассмотрены основные способы его совершения и меры защиты от последней.

Summary. The thesis analyzes such a type of cybercrime as social engineering. The main methods of its commission and measures of protection against the latter are considered.

Напевно, сьогодні вже неможливо уявити життя кожного з нас без використання інформаційних технологій. Кожен із нас дедалі більше використовує віртуальну сферу для збереження важливої інформації. Роботизація та автоматизація виробничого процесу повинна бути спрямована на полегшення та покращення життя та здоров'я працівників, зокрема шляхом зменшення робочих місць у небезпечних, шкідливих та важких умовах праці, що вимагає відповідних змін до трудового законодавства [1].

Кіберзлочини найчастіше ставлять під загрозу не лише приватну сферу, а й життєво важливу інфраструктуру, яка в багатьох країнах не контролюється публічним сектором, і такі злочини можуть чинити дестабілізуючий вплив на всі верстви суспільства. З розвитком технологій «в ногу» розвивається і злочинність у даній сфері, яка дістала назву кіберзлочинність. Кіберзлочинці використовують різноманітні методи і способи вчинення злочинів у віртуальному просторі, одним з яких є соціальна інженерія.

Зазначене явище є досить розвинутим як в Україні, так і за її межами, адже кожному з нас приходять повідомлення на кшталт - «Цього разу саме ви виграли автомобіль! Вітаємо». Під соціальною інженерією розуміють певну методику впливу на людей (маніпулювання), котра змушує останніх віддавати злочинцям цінну інформацію. В основі соціальної інженерії лежить маніпулювання людьми, а саме їх довірою, страхом або цікавістю.

Темпи зростання кількості злочинів, що здійснюються в цій сфері, збільшуються пропорційно кількості користувачів комп'ютерних мереж і, за оцінками Інтерполу, є найшвидшими на планеті [2].

Для ефективної боротьби з соціальною інженерією необхідно детально вивчити основні способи її вчинення. До них можна віднести наступні:

Фішинг – це схема, за якою хакери змушують користувачів передавати конфіденційну інформацію, наприклад, паролі та номери соціального страхування. Зазвичай вона передбачає надсилання користувачеві повідомлення, яке ніби походить із вартого довіри джерела, наприклад, із банку (це наживка). У повідомленні міститься посилання на шахрайський webсайт, що видається за варте довіри джерело (це пастка). Користувач спокійно вводить інформацію, яка цікавить хакерів, вважаючи, що перебуває на безпечному сайті [3]. На сьогодні така схема соціальної інженерії користується великою популярністю.

Вішинг – полягає в імітації дзвінків на мобільний телефон від ніби то банківської установи для підтвердження певної інформації. При такій схемі шахрайства, особа отримує певну вимогу розповісти конфіденційну інформацію, або наприклад назвати свій пароль, який у майбутньому буде використаний для доступу до банківського рахунку.

Фармінг – полягає у перенаправленні особи на невірну IP-адресу. Тобто злочинець певним чином встановлює на комп'ютер шкідливу програму яка після її запуску перенаправляє особу на підроблені сайти замість потрібних останній. Такий вид шахрай-

ства часто зустрічається при завантаженні певних програм з неналежних сайтів.

«Дорожнє яблуко» - полягає у здійсненні шахрайства за допомогою використання фізичних носіїв інформації. Так, особа злочинець може залишити флеш-носій, CD-диск із таким зображенням у певному публічному місці, скажемо кафе, яке в свою чергу може викликати цікавіть в особи, і як результат вона забажає переглянути його у себе на комп'ютері.

Зворотна соціальна інженерія має місце лише в тому випадку, коли злочинець безпосередньо знайомий із особою та певним чином отримав її довіру або заслуговує на неї. За таких обставин, жертва сама звертається до особи з проханням надати їй допомогу у виконанні певної роботи.

«Плечовий серфінг» в свою чергу дає можливість отримати особисту інформацію від жертви шляхом підглядання за діями користувача через його плече, зокрема спостереження за тим, як людина друкує на клавіатурі свого комп'ютера, щоб виявити й вкрасти її пароль або іншу призначену для користувача інформацію [4].

Такий перелік способів вчинення соціальної інженерії звісно ж не є повним і сталим, оскільки кожного дня злочинці за допомогою своїх «інтелектуальних» здібностей, розширюють способи і методи вчинення злочинів у віртуальній сфері. Чимало людей поводяться віктимно у повсякденному житті і при цьому не стають жертвами злочинів. Більш того, одна і та ж віктимна поведінка за різних обставин призводить до різних наслідків [6].

Існують певні сталі ознаки, за допомогою яких на теперішній час можна визначити соціальну інженерію. До них зокрема відносяться такі:

Поганий правопис, відсутність граматики;

Сумнівна адреса відправника. Це зумовлено тим, що переважно злочинці не витрачають багато часу на створення доменного імені;

Наявна терміновість. Може виражається такими словосполученнями як «терміново надішліть нам свої дані». Це в першу чергу необхідно для того, щоб особа не встигла подумати і зрозуміти що ж відбувається;

Запити на інформацію яка є конфіденційною. Працівники банку не будуть питати у вас останні цифри вашої картки та пін код від неї;

Звучить занадто добре. Це стосується в першу чергу всіх розіграшів автомобілів та інших подібних СМС, де кожен із нас фактично кожного дня виграє ледь не по мільйону гривень.

Отже, підсумовуючи вище наведена, варто сказати, що злочини у сфері соціальної інженерії є досить поширеними в світі. Варто наголосити, що нормативно-правова база у сфері регулювання розвитку інформаційного суспільства і заходи щодо формування державної інформаційної політики мають повною мірою узгоджуватися із завданнями в сфері інформаційної безпеки, практикою забезпечення збереження державної таємниці, захисту інформаційно-телекомунікаційної інфраструктури та інформаційних ресурсів від кібератак й інших загроз в інформаційному просторі [8]. Для запобігання вчиненню злочинів у даній сфері, необхідно дотримуватися простих правил захисту цінної інформації, таких як встановлювати надійні паролі та не переходити на сумнівні сайти. Також з метою захисту великих компаній від соціальної інженерії, можна запровадити регулярне навчання для працівників стосовно питань кібербезпеки та проявів соціальної інженерії.

ЛІТЕРАТУРА:

1. Robotization of manufacturing process: economic and social problems and legal ways of their solution / O. E. Kostyuchenko, T. V. Kolesnik, Z. V. Bilous, O. V. Tavolzhanskyi // Financial and credit activity: problems of theory and practice. – 2019. – Vol. 3, is. 30. – P. 454–462.

2. Орлов О. В., Онищенко Ю. М. Попередження кіберзлочинності – складова частина державної політики в Україні. Теорія та практика державного управління. 2014. Вип. 1 (44). С. 9–15. Режим доступу: http://nbuv.gov.ua/UJRN/Tpdu_2014_1_4

3. Сайт «GoDaddy»: Що таке фішинг? [Електронний ресурс]. – Режим доступу: https://ua.godaddy.com/help/sho-take-fishing-346 .

4. Сайт «Um.co.ua»: Плечовий серфінг [Електронний ресурс]. – Режим доступу: http://um.co.ua/4/4-5/4-57341.html .

5. Tsypko, Victoria, Kateryna I. Alieksieieva, Iryna A. Venger, Oleksii V. Tavolzhanskyi, Nataliya I. Galunets, & Alona V. Klyuchnik. « Information Policy of the Enterprise as the Basis for the Reproduction of Human Potential in the Structure of Public Social Interaction.» Journal

of Advanced Research in Law and Economics [Online], 10.6 (2019): 1664-1672. Web. 6 Nov. 2020

6. Головкін Б. М. Як стають жертвами злочинів // Проблеми законності. Вип. 136. 2017. С. 161 – 172. URL: http://nbuv.gov.ua/UJRN/Pz_2017_136_19

7. Ovcharenko, Mykola O; Tavolzhanskyi, Oleksii V; Radchenko, Tetiana M; Kulyk, Kateryna D; Smetanina, Nataliia / Combating Illegal Drugs Trafficking Using the Internet by Means of the Profiling Method /Tavolzhansky O. V.// V.Journal of Advanced Research in Law and Economics; Craiova Том 11, Изд. 4(50), (Summer 2020): 1296-1304.

8. Кримінологія : підручник / Б. М. Головкін, В. В. Голіна, О. Ю. Шостко та ін.; за ред. Б. М. Головкіна. – Харків : Право, 2020. – С. 252.

9. Tavolzhanskyi, O.V. (2017). Osnovu derzhavnoi kiberpolituku Ukrainu: formuvannya ta realizatsiya. Naykovo-informatsyinui visnuk Ivano-Frankivskogo yniversutety prava imeni Korolya Danula Galutskogo: Seriya Pravo, 4. (16), 158–164 [In Ukrainian].

Науковий керівник доц., к.ю.н. О.В. Таволжанський