УДК 004.056.53

В.В. Вишньовський
Л.М. Ткачук

СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК ЗАСІБ ВПЛИВУ НА ЛЮДСЬКУ СВІДОМІСТЬ

Вінницький національний технічний університет;

Анотація
Проведенно огляд понять соціальна інженерія як засіб впливу на людську свідомість. Наведено різновид соціальної інжинерії, які значно впливають на людину.
Ключові слова: *Соціальна інженерія, фішинг, листи, емоційна буря, людська свідомість, атака*
Abstract: *A review of the concepts of social engineering as a means of influencing human consciousness is carried out. A variety of social engineering that has a significant impact on a person is given.*
Keywords: *Social engineering, phishing, letters, emotional storm, human consciousness, attack*

Вступ

Людська свідомість є невідємною частиною у формувані суспільства. В сучасному світі вона має свій темний бік, який має назву соціальна інженерія - сукупність методів, основаних на психологічних особливостях людей: цікавість, довіра, звичка тощо [1].

Метою соціальної інженерії є спонукання людей робити певні дії, які вони за звичних умов ніколи не вчинили, наприклад, розголошувати власну конфіденційну інформацію, переходити на невідомі сайти та за сумнівними посиланнями. Вся система соціальної інженерії базується на тому факті, що саме людина є найслабкішою ланкою будь-якої системи інформаційної чи кібербезпеки. Саме тому, якщо інформацію технічними засобами отримати дуже важко (паролі, адеса проживання, тощо), то можна вплинути безпосередньо на людину, яке є найслабкішим місцем в системі інформаційної безпеки.

Результати дослідження

Соціальна інженерія виконує як інструментальні функції так і стабілізуючі і управлінські. Цілі соціальної інженрії формулюються і визначаються, як правило, замовником – державними або приватними організаціями, які фінансують і визначають соціальне замовлення, тобто його напрямок і результати [2].

Особливе значення соціальна інженерія надає психологічним факторам і засобам впливу (методи соціометрії, психодрами, соціодрами, соціально-психологічного тренінгу тощо).

Занадто довірливі користувачі досить легковажно відносяться до власної кібербезпеки і не усвідомлюють, що неуважність може коштувати їм значних фінансових втрат. Для цього кібершахраї використовують особливі методи соціальної інженерії, які розраховані на різні аспекти людської психології. Також цими же методами можна маніпулювати будь-якою людиною, яку вивели з рівноваги [3].

Фішинг є одним з видів соціальної інженерії. Суть методу полягає у створенні підробленої сторінки сайту банку чи іншої установи з метою «витягування» у користувача логіну та паролю від його акаунта. Це дасть можливість зловмисникам, перевести всі гроші з банківського рахунку жертви на власний або розповюдження вірусів та іншого щкідливого програмного забезпечення через завантаження різного роду скриптів. Частіше за все, фішинг розрахований на неуважних користувачів, які не звертають уваги на незвичайні назви сайтів, частіше за все з помилками, незвичайний зовнішній вигляд знайомих ресурсів та нехтують основним правилами сучасної кібербезпеки.

Для прикладу, оригінальна адреса відомого в Україні онлайн-банку - privat24.ua, фішингова сторінка може мати тільки одну неправильну літеру або схожу назву та бути витриманою у корпоративних кольорах компанії - priwat24.ua

Листи від банків. Розповсюдженим методом соціальної інженерії є, так звані, «листи від банків». Суть методу дещо інша ніж класичний фішинг. Фактично, зловмисники не чекають поки користувачі самі потраплять на підроблений сайт, а самі спонукають їх це зробити. Це здійснюється за допомогою фальшивих повідомлень від банків чи інших установ.

«Емоційна буря». Найяскравішим прикладом соціальної інженерії є так звані «WOW-повідомлення». Це «гра» на природній цікавості та емоційності користувачів. Вони мають вигляд коротких повідомлень від друзів на пошту, у соцмережах, месенджерах, зміст яких має спонукати перейти за посиланням у тілі повідомлення. «ОГО! Подивись яка прикольна річ. Я був у шоці!» - класичний приклад такого методу соціальної інженерії. Посилання можуть вести як на фішингові сайти, так і на автоматичне завантаження шкідливого програмного забезпечення, яке також буде використано для крадіжки конфіденційної інформації із зараженого комп'ютера [4].

Протидія соціальній інженерії схожа на внутрішню боротьбу з людською суттю. Є декілька правил, які допоможуть не попадатись на гачки шахраїв.

Перш за все, необхідно звертати увагу на написання адрес сайтів.

Якщо на електрону адресу прийшов лист та настирливо пропонує переглянути сайт,фото або відео, зазиваючи емоційними закликами, то переходити не рекомендується.

Вводячи логін та пароль в акаунтах на сайтах, необхідно звертати увагу на незвичайні зміни зовнішнього вигляду сторінок. Якщо щось викликає підозру, то краще перевірити оригінальність ресурсу ще раз.

Ці правила не є вичерпними, але тримаючи їх у пам'яті та використовуючи як фільтр під час користування інтернетом, можна суттєво покращити свій інформаційний захист та стати менш вразливим до методів соціальної інженерії.

Висновки

Таким чином, соціальна інженерія є досить актуальною проблемою, яка впливає на людську свідомість. Проблема довірливості людей є найслабшою ланкою в будь-якій системі, не залежно від механізмів захисту. Перед відкриттям будь-якого листа отриманого по електроній адресі, першим етапом необхідно переконатися у правильності адреса відправника і вміст повідомлення. Також необхідно звертати увагу на прикріплені файли у повідомлені.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кевин Митник. Искусство обмана [Електронний ресурс] - Режим доступу: http://rulit.me/books/ iskusstvo-vtorzheniya-read-16566-1.html
2. Соціальна інженерія [Електронний ресурс] - Режим доступу: http://studies.in.ua/lekcii-sociologija/4443-socalna-nzhenerya.html
3. СОЦІАЛЬНА ІНЖЕНЕРІЯ - МЕТОДИКА МАНІПУЛЮВАННЯ ШИРОКИМИ МАСАМИ ЛЮДЕЙ [Електронний ресурс] - Режим доступу: http://uk.ruarrijoseph.com/obschestvo/ 72810-socialnaya-inzheneriya-metodika-manipulirovaniya-shirokimi-massami-lyudey.html
4. Кевин Д. М., Вильям Л. С., Искусство вторжения / Д. Кевин - Издательский дом «Альпина Паблишер», Москва, 2012. – 36 с.

Вишньовський Владислав Васильович — студент групи 1БС-17м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, Україна, e-mail: vyshnovskyi@outlook.com

Науковий керівник:

Ткачук Людмила Миколаївна — к.е.н., доцент кафедри інтеграції навчання з виробництвом, Вінницький національний технічний університет, м. Вінниця, Україна

Vyshnovskyi Vladyslav — Student of Information Technologies and Computer Engineering Department, Vinnytsia National Technical University, Vinnytsia, Ukraine, e-mail: vyshnovskyi@outlook.com

Supervisor:
Tkachuk Lyudmila **—** PhD, Associate Professor of the Department of Integration of Education with Production, Vinnytsia National Technical University, Vinnytsia, Ukraine