2. Кулик О. Кримінологічний аналіз злочинності в Україні: напрями вдосконалення методології та методики. *Право України*. 2009. № 7. С. 52-57.

3. Бесчастний В. М. Методи інформаційного забезпечення як інструментарій збору та обробки інформації про злочинність. *Право і суспільство*. 2017. № 1. С. 206-212.

4. Орловська Н. А. Щодо ефективності запобігання транснаціональній торгівлі людьми // Протидія незаконній міграції та торгівлі людьми : матер. ІІ Міжнар. наук.-практ. симпозіуму (м. Івано-Франківськ, 16-17 бер. 2018 р.). Ів.-Франк. : Редакц.-видавн. відділ Університету Короля Данила, 2018. С. 105-109.

5. The Global Slavery Index. URL: https://www.globalslaveryindex.org/2018 (дата звернення: 31.10.2018).

Одержано 31.10.2018

УДК 343.72

Ярослав Віталійович ОСІПОВ,
курсант 3 курсу групи Ф4-302 факультету № 4 (кіберполіції) Харківського національного університету внутрішніх справ;
Денис Олександрович ГРИЩЕНКО,
старший викладач кафедри кібербезпеки факультету № 4 (кіберполіції) Харківського національного університету внутрішніх справ

СПОСІБ ШАХРАЙСТВА ЗА ДОПОМОГОЮ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Соціальна інженерія – це психологічна експлуатація, яку шахраї використовують, щоб вміло маніпулювати людськими слабкостями та здійснювати емоційні напади на невинних людей. Соціальна інженерія використовується найчастіше за допомогою фішингу (фішинг – це схема, за якої хакери змушують користувачів передавати конфіденційну інформацію, наприклад паролі та номери соціального страхування). Ці фішингові електронні повідомлення, як правило, супроводжуються загрозливим тоном через терміновість. Оскільки малоймовірно, що Інтернет-шахрайство буде повністю ліквідовано, найважливішою стратегією, яка може бути спрямована на боротьбу з нападом соціальної інженерії, є інформування громадськості про можливі загрози від злочинців.

Люди стають жертвами шахрайства, оскільки вони невірні, наївні чи жадібні. Соціальні інженери можуть використовувати слабкі сторони для отримання бажаної поведінки та надання доступу до інформації через психологічно побудовані комунікації. Ці шахраї можуть вміло маніпулювати жертвами в емоційно вразливому стані з замаскованою, привабливою електронною поштою. Суворість та наслідки інтернет-шахрайства вимагають аналізу такого роду злочинів. За даними Consumer Senteninel (Федеральна торгова комісія США), споживачі подали 221,226 скарги на шахрайство, пов'язане з Інтернетом. Повідомлення електронної пошти відіграє важливу роль в

інтернет-злочинах. Електронна пошта є найчастішим контактним методом, що використовується винуватцями інтернет-шахрайства. Емоційний вплив та тривалі наслідки для жертв, під час комп'ютерного шахрайства, також можуть бути серйозними. Федеральна торгова комісія повідомила, що 31% жертв особистих крадіжок, які отримали кредитні картки на їх ім'я, вимагали понад 40 годин для виправлення кредитних проблем та таких наслідків, як переслідування кредиторів (48%), відмови від позик (25%), а також кримінальні справи (12%). За даними, отриманими від Центру інтернет-кримінальних злочинів, середня втрата на одну жертву була найвищою серед шахрайства (3000 доларів), довірчого шахрайства (2000 доларів США) та шахрайства з авансовими платежами (1650 доларів США). У одному рідкісному випадку британець кінчив життя самогубством, ставши жертвою шахрайських дій з відмивання грошей використовуючи мережу Інтернет (BBC News, 2004).

Термін «соціальна інженерія» передбачає процес обману людей у видачі конфіденційної інформації. Соціальні інженери – люди, які навмисно вводять в оману та маніпулюють людьми на особисту користь. Атаки соціальної інженерії можуть відбуватися на корпоративному або індивідуальному рівні. Найбільш поширеними місцями для інженера-соціальника, який шукає незаконну інформацію та доступ до психологічного нападу, включає робоче місце, телефон, сміттєві баки та Інтернет. Психологічні напади зосереджені на переконаннях та доброзичливості.

Існує багато методів соціальної інженерії в залежності від середовища, для її реалізації. Середовищем може бути електронна пошта, веб, телефон, USB-накопичувачі або інше. Отже, є такі типи:

1. Фішинг. Зловмисник відтворює веб-сайт або портал підтримки відомої компанії та надсилає посилання на цілі за допомогою електронної пошти або соціальних медіа-платформ. Інша особа, зовсім невідома реальний ризик, призводить до компрометації особистої інформації та навіть даних про кредитні картки. Ви можете запобігти фішинговим електронним листам, використовуючи спам-фільтри у облікових записах електронної пошти. Крім того, не відкривайте електронні листи, що надходять з ненадійного джерела або має вигляд підозрілої.

2. Вішинг. Імпульси або соціальні інженери можуть бути в будь-якому місці в Інтернеті. Але багато хто віддає перевагу старовинному шляху; вони використовують телефон. Цей тип атаки соціальної інженерії відомий як Вішинг. Вони відтворюють систему IVR (Interactive Voice Response) компанії. приєднуючись до безкоштовного номера змушують людей телефонувати та вводити свої дані.

3. Претексування – це ще один приклад соціальної інженерії. Вона заснована на скриптовому сценарії, представленому перед цілями, які використовуються для вилучення деякої іншої інформації. Зловмисник може видати себе за іншу особу або відомої фігури. Можливо, ви

бачили різні телевізійні шоу та фільми, де детективи використовують цю техніку, щоб потрапити в місця, де вони особисто не авторизовані, або отримати інформацію, обдурюючи людей. Іншим прикладом попередження може бути підроблені електронні листи, які ви отримуєте від своїх віддалених друзів, які потребують грошей. Можливо, хтось зламав свій обліковий запис або створив фальшивий.

4. Приманка. Цифровий варіант цієї методики відомий як "Байтинг", і це одна з методів соціальної інженерії, що використовуються людьми. Зловмисники залишають заражені USB-накопичувачі або оптичні диски у громадських місцях, сподіваючись, що хтось вибере його з цікавості та використовуватиметься на своїх пристроях. Більш сучасний приклад приманки можна знайти в Інтернеті. Різні посилання на завантаження, в основному містять шкідливе програмне забезпечення, кидаються перед випадковими людьми, які сподіваються, що хтось натискає на них.

5. Інший метод соціальної інженерії *Quid pro quo* містить в собі людей, що ставлять як технічну підтримку. Вони роблять випадкові дзвінки співробітникам компанії, які заявляють, що вони зв'язані з ними стосовно проблеми. Іноді такі люди отримують шанс зробити жертву робити те, що вони хочуть. Його також можна використовувати для повсякденних людей. *Quid pro quo* передбачає обмін чимось з ціллю, наприклад, зловмисник, який намагається вирішити справжню проблему жертви. Обмін може включати матеріальні речі, такі як подарунок за інформацію.

Як захистити себе від соціальних інженерів?

Ви повинні бути насторожені, коли хтось просить вас надати вашу інформацію або коли якась незнайома людина щось дає вам безкоштовно. Є деякі правила безпеки, щоб не стати жертвою соціальних інженерів:

– зберігайте свої облікові записи та пристрої в безпеці;
– подумайте перед тим, як діяти;
– покращити свій емоційний інтелект;
– забудьте про своє оточення;
– нікому не давати свою конфедиціальну інформацію;
– не відповідати на СМС-повідомлення з неперевірених джерел.

Висновок. Небезпека нападів соціальних інженерів полягає у відсутності будь-якої системності та загального сценарію їх дій. Єдине, що точно визначено – це ціль – людина. Основою даного методу є використання людського фактора, як найбільш незахищеного елемента будь-якої відкритої системи, якими на сьогодні є усі підприємства. Теоретично абсолютний захист системи можливий при абсолютному виключенні людини із цієї системи та побудова несистемного алгоритму даної системи.

Список бібліографічних посилань

1. Резник Ю. М. Социальная Инженерия как профессия. *Известия томского политехнического университета*. 2011. Т. 318. № 6. С.124-130. URL:

https://cyberleninka.ru/article/v/sotsialnaya-inzheneriya-kak-professiya (дата звернення: 30.10.2018).

2. Ногалес К. Социальная инженерия // 4brain. 12 Дек 2017. URL: https://4brain.ru/blog/социальная-инженерия/ (дата звернення: 30.10.2018).

3. Bezmaly V. Как защищать сотрудников от угроз социальной инженерии // IT-community: IT сообщество Украины. 23.07.2014. URL: https://it-community.in.ua/2014/07/kak-zashhishhat-sotrudnikov-ot-ugroz-sotsialnoj-inzhenerii.html/ (дата звернення: 30.10.2018).

4. Bezmaly V. Технологи социальной инженерии // IT-community: IT сообщество Украины. 29.10.2014. URL: https://www.it-community.in.ua/2014/10/tehnologi-sotsialnoj-inzhenerii.html/ (дата звернення: 30.10.2018).

5. Нам'ясенко В. М. Соціальна інженерія як одна із загроз економічній безпеці, що спричиняє негативний вплив на ефективність діяльності підприємства. *Економіка та держава*. 2016. № 3. С. 90-92. URL: http://www.economy.in.ua/pdf/3_2016/21.pdf (дата звернення: 30.10.2018).

6. Соціальна інженерія (безпека) // Вікіпедія: вільна енциклопедія. URL: https://uk.wikipedia.org/wiki/Соціальна_інженерія_(безпека) (дата звернення: 30.10.2018).

Одержано 31.10.2018

УДК 681.3.06

Артур Геннадійович ПЛАКСЮК,
курсант 2 курсу групи Ф4-202 факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ

ПРОБЛЕМАТИКА ЗАХИСТУ ІНФОРМАЦІЇ В БАЗІ ДАНИХ

Можна з достовірністю стверджувати, що більшість прикладних програм, які призначені для виконання будь-якої корисної роботи, тим або іншим чином використовують структуровану інформацію або, іншими словами, упорядковані дані. Такими даними можуть бути, наприклад, списки замовлень на той чи інший товар, списки пред'явлених і оплачених рахунків, список телефонних номерів ваших друзів, або розклад руху автобусів у вашому місті .

При комп'ютерній обробці інформації, упорядковані будь-яким способом, дані зберігаються в базах даних (БД) – особливих файлах, використання яких разом із спеціальними програмними засобами дозволяє користувачеві переглядати необхідну інформацію, так само, як і при необхідності, маніпулювати нею, наприклад, додати, змінити, копіювати, видалити, сортувати і т.д. Просто кажучи, дати визначення бази даних можна наступним чином: база даних – це набір інформації, організованої будь-яким способом.

В сучасному світі жодна організація, підприємство і т.д. не обходиться без використання БД які містять найрізноманітнішу інформацію. Таким чином в БД може зберігатися дуже делікатна або