УДК 004.056

Гуралюк А.Г.
кандидат педагогічних наук, старший науковий співробітник, завідувач сектору ІКТ і наукометрії відділу наукового інформаційно-аналітичного супроводу освіти Державна науково-педагогічна бібліотека України імені В. О. Сухомлинського НАПН України

СОЦІАЛЬНА ІНЖЕНЕРІЯ ТА ЗАХИСТ ВІД НЕЇ

З моменту появи комп'ютерів і початку розвитку Інтернету програмісти усіма силами прагнуть забезпечити комп'ютерну безпеку. Проте, якою б серйозною не була система захисту, залишається слабка ланка – людина, особливо, якщо ця людина довірлива, наївна і психологічно нестійка.

Соціальна інженерія – методи психологічного маніпулювання людиною, що змушують її робити те, що вона робити не збиралась.

Як правило, сучасні кіберзлодії переслідують дві основні мети: крадіжку паролів і установку шкідливого програмного забезпечення. Зловмисники користуються соціальною інженерією за допомогою телефону, електронної пошти, соціальних мереж, месенджерів тощо.

Способи, якими кібершахраї виманюють певні ресурси (гроші, паролі, конфіденційні дані, секретну інформацію тощо), насправді, існує не так багато. Вони всі пов’язані із так званими когнітивними упередженнями. Деякими шаблонами, що притаманні людському мозку і, в цілому, допомагають в різних життєвих ситуаціях. Так, наприклад, при пожежі ми кидаємось спасати щось найцінніше, тому коли шахрай увімкне пожежну сигналізацію, ми мимоволі, викажемо де у нас це найцінніше заховано.

Опишемо декілька найбільш типових прийомів соціальної інженерії.

1. «Емоційна буря». Як правило, для жертви все починається із «WOW- повідомлення». Воно може мати вигляд короткого повідомлення від друзів на пошту, у соцмережу чи месенджер, зміст якого має спонукати перейти за посиланням на сайт шахрая. Класичний приклад: «Мережі вайбер 10 років! Пройдіть коротку анкету і отримайте невеличкий подарунок!». Такі посилання можуть вести як на фішингові сайти, так і на автоматичне завантаження шкідливого ПЗ, що також буде використано для крадіжки конфіденційної інформації з зараженого ПК [2] .

2. Фішинг (fishing) – виманювання у довірливих або неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів з переказу або обміну валюти, інтернет-магазинів. Шахраї намагаються змусити користувачів самостійно розкрити конфіденційні дані, наприклад, надсилаючи електронні листи із пропозиціями підтвердити реєстрацію облікового запису, що містять посилання на веб-сайт в інтернеті, зовнішній вигляд якого повністю копіює дизайн відомих ресурсів.

Це один з різновидів соціальної інженерії, заснований на незнанні користувачами основ мережевої безпеки. Зокрема, багато хто не знає простого факту: сервіси не розсилають листів з проханнями повідомити свої облікові дані, пароль та інше.

3. «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, в тексті яких міститься інформація на зразок:

- залякувань втратою грошей;
- можливості отримання виграних в псевдо-акціях призів;
- вимог уточнення інформації.

Всі ці «пропозиції» закінчуються проханням передати особисті коди доступу шахраям. Це може бути запрошення перейти на сайт зовні схожий на сайт банку, де треба буде заповнити реквізити банківської карти, чи встановити на свій гаджет додаткове програмне забезпечення тощо.

4. Прітекстінг (Pretexting) –отримання інформації або спонукання до вчинення певних дій обманом на основі заздалегідь складеного сценарію або створення фіктивної ситуації. Застосовується через телефон та потребує проведення попередніх досліджень для входження в довіру.

5. Тайпсквоттинг (typosquatting). Ця техніка грунтується на тому, що люди роблять помилки під час набору адрес в браузері. Відповідно, під час помилкового введення, жертва може бути перенаправлено на сайт, створений

зловмисником. Спочатку кіберзлодії зважено готують базу для реалізації цієї схеми. Прикидають варіанти помилок і створюють сайт, як дві краплі води схожий на легітимний. Таким чином, помилка в одному символі може привести вас на копію, мета якої - збір персональних даних або поширення шкідників [1].

Це далеко не повний перелік методів соціальної інженерії. Для боротьби із нею потрібно у першу чергу спиратись на здоровий глузд. Декілька найпростіших порад:

- звертайте увагу на написання адрес сайтів;
- якщо Вам пропонують переглянути сайт/фото/відео, зазиваючи емоційними закликами – не переходьте, можливо це приклад соціальної інженерії.
- вводячи логін/пароль в акаунтах на сайтах, звертайте увагу на незвичайні зміни зовнішнього вигляду сторінок. Якщо щось викликає підозру – краще перевірити оригінальність ресурсу ще раз;
- критично ставтесь до електронних листів, а особливо до посилань за якими пропонують перейти незнайомі відправники повідомлень [2].
- не використовуйте один і той же пароль для доступу до зовнішніх і корпоративних ресурсів;
- блокуйте комп'ютер, коли не перебуваєте на робочому місці;
- встановіть антивірус;
- обговорюйте по телефону і в особистій розмові тільки необхідну інформацію;
- видаляйте всі конфіденційні документи з портативних пристроїв.

Використані джерела

1. Самые популярные методы социальной инженерии в 2018 году. Информационный портал SecurityLab.ru. Доступ: https://www.securitylab.ru/analytics/498784.php
2. Соціальна інженерія або маніпуляції свідомістю. Офіційний сайт антивірусної лабораторії Zillya! . Доступ: https://zillya.ua/sotsialna-inzheneriya-abo-manipulyatsi-svidomistyu
3. Цуркан, О. Методи протидії використанню соціальної інженерії / Оксана Цуркан, Ростислав Герасимов, Ольга Крук // Information Technology and Security. – 2019. – Vol. 7, Iss. 2 (13). – Pp. 161–170. – Bibliogr.: 11 ref. Доступ: https://ela.kpi.ua/bitstream/123456789/33885/1/ITS2019-7-2_05.pdf
4. Методы социальной инженерии, или атаки на человеческий фактор. Офіційний сайт компанії a1qa . Доступ: https://www.a1qa.ru/blog/sotsialnaya-

inzheneriya-ili-ataki-na-chelovecheskiy-faktor/