Одеський державний університет внутрішніх справ
Кафедра кібербезпеки та інформаційного забезпечення
Факультет підготовки фахівців для підрозділів кримінальної поліції

КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ

International scientific-practical conference
"Cybersecurity in Ukraine: Legal and Organization Issues"

Матеріали
Міжнародної науково-практичної конференції
19 листопада 2021 року

Одеса 2021

Рекомендовано до друку рішенням кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ
(протокол № від грудня 2021 року)

Всі матеріали надані в авторській редакції та виражають
персональну позицію учасника конференції

Кібербезпека в Україні: правові та організаційні питання: матеріали міжн. наук.
К38 практ. конф., м. Одеса, 26 листопада 2020 р. Одеса : ОДУВС, 2021. _____ с.
ISBN 678-717-7020

У збірнику представлено стислий виклад доповідей і повідомлень, поданих на міжнародну науково-практичну конференцію «Кібербезпека в Україні: правові та організаційні питання», яка відбулася на базі кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ 19 листопада 2021 року.

У матеріалах конференції приділено увагу актуальним теоретичним та практичним проблемам забезпечення інформаційної безпеки в Україні. Висвітлюється широкий спектр питань, пов'язаних з удосконаленням правового регулювання та адміністративно-правового забезпечення кібербезпеки в Україні. Розглянуто використання інформаційних систем, технологій та інформаційно-аналітична діяльність правоохоронних підрозділів у боротьбі з злочинністю та надано обґрунтовані рекомендації щодо вдосконалення підготовки персоналу для боротьби з кіберзлочинністю в Україні.

Матеріали всеукраїнської науково-практичної конференції адресовано вченим, працівникам правоохоронних органів, аспірантам (ад'юнктам), слухачам магістратури, студентам та курсантам вищих навчальних закладів.

ФІШИНГ - НАЙПОШИРЕНІШИЙ ВИД КІБЕРШАХРАЙСТВА

Ротарь Л.М.
курсантка 202 взводу ФПФКП ОДУВС
Форос Г.В.
т.в.о завідувача кафедри кібербезпеки та інформаційного забезпечення ОДУВС
к.ю.н., доцент

Одна з головних цілей фішингу - «вивудити» конфіденційні дані жертви та заробити на них: продати конфіденційну інформацію або використовувати її для отримання коштів користувача.

Технічні засоби для боротьби з фішингом існують уже давно, але вони не завжди працюють ,про це свідчить поширеність цього злочину

Найкращий спосіб захистити себе від фішингових атак – навчитися їх розпізнавати. А для цього варто вивчити їхню структуру та принцип роботи.

Фішинг можна розділити на дві основні категорії: звичайний та цільовий. Перший - масовий, відрізняється широким охопленням і зазвичай має вигляд спам-кампаній. Такий вид фішингу часто називають безадресним.

У випадку з цільовим фішингом мішенню стають строго певні люди або невеликі групи пов'язаних між собою осіб.

Безадресний фішинг

Напевно, кожен із нас стикався з ним. У своїй теці зі спамом можна знайти десятки подібних листів. Дізнатися їх порівняно просто: такі повідомлення часто містять помилки та граматичні помилки, та й загалом виглядають непрофесійно.

Цільовий фішинг використовує складніші схеми, ніж звичайний. Найчастіше він технологічніший, а можливі збитки більші. Зловмисники вивчають своїх жертв та їх профілі в соціальних мережах, збирають інформацію про їхні звички, використовувані сервіси, контакти та багато іншого. Якщо використовувати ці дані при складанні листа, він виглядатиме переконливим і правдоподібним.

Через уявну багатьом простоту безадресного фішингу багато хто впевнений, що зловити їх на подібні хитрощі неможливо. Це дає почуття хибної безпеки.

Користувачі стають жертвами фішингових атак через поєднання структури листа, обману, що міститься в ньому, і різних емоційних тригерів, які зловмисники використовують для отримання необхідної відповіді. Про них ми розповімо далі. Розуміючи принципи фішингу, набагато простіше його розпізнати.

Структура фішингової атаки

Розглянемо приклад фішингу електронною поштою, оскільки такі атаки найбільш поширені і дозволяють повністю розібратися в роботі шахрайських повідомлень.

Видимий заголовок листа

Видимий заголовок листа — це частина електронного повідомлення, яку ми бачимо, перш ніж його відкриємо. Це перша можливість для зловмисників привернути вашу увагу, але саме тут провалюється багато безадресних кампаній.

Метою масових розсилок цьому етапі є спроба викликати інтерес і імітувати надійне джерело. В адресі відправника може бути вказана назва вашого банку.

Переконливий текст

Текст шахрайського листа містить у собі «приманку». Якщо зловмисники переконали жертву відкрити лист, його текст повинен змусити зробити необхідну дію - завантажити файл, перейти за посиланням або надіслати дані. Зазвичай у своїй використовується безліч емоційних прийомів, щоб завоювати довіру користувача.

Шкідливий вміст

Шкідливий вміст – ключовий компонент фішингового листа. Найбільш поширеним видом такого вмісту є шкідливе посилання. Вона може вести на «заражений» чи підроблений сайт. Введені на ньому облікові дані опиняться у руках зловмисників. Таке посилання може бути як у тексті листа, і у вкладенні.

Емоційні тригери

Заголовок, тема, приманка та шкідливий вміст – це основа фішингового повідомлення, але успіх чи провал атаки залежить від емоційних тригерів, які в ньому містяться. Вони мають спровокувати негайну, необдуману, машинальну реакцію.

Жадібність

Напевно, жадібність – перший емоційний тригер, який почали використовувати у фішингових схемах. Його застосовували навіть до сумнозвісних «листів від нігерійського принца», але спроби нажитися на чужій жадібності не припиняються до цього дня.

Терміновість

Часто фішинг тисне і на стислий термін. Саме собою відчуття терміновості не надто ефективно, тому його необхідно поєднувати з іншими емоційними тригерами. "Ви можете безкоштовно отримати подарунок, але його потрібно забрати протягом 24 годин".

Страх

Страх може використовуватись у безлічі різних ситуацій. Він часто застосовується разом із терміновістю, особливо коли жертву лякають негативними наслідками, якщо вона не відповість негайно. Страх у поєднанні із терміновістю часто породжує паніку. Їх використовують у погрозах, пов'язаних із притягненням до юридичної відповідальності або розповсюдженням інтимних особистих даних

Співчуття

Більшість емоційних тригерів пов'язані з нашими базовими інстинктами, але шахраї можуть скористатися і позитивними рисами нашого характеру.

Цікавість

Цікавість може бути особливо небезпечним тригером. Адже ми часто думаємо, що нічого серйозного не станеться, якщо «глянути одним оком». У фішингу можуть застосовуватися ті самі принципи, що й у клікбейтні статті в інтернеті.

Література:

1. Що таке фішинг і як захиститися від шахраїв в мережі. Режим доступу: https://volnovakha.city/articles/88782/scho-take-fishing-i-yak-vberegti-svoi-dani-v-merezhi
2. Фішинг у соціальних мережах набирає обертів Режим доступу: https://i.factor.ua/ukr/journals/bk/2010/february/issue-3/article-100704.html