Правительство Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский университет «Высшая школа экономики»

Кафедра «Компьютерная безопасность»

План подготовки к проведению эксперимента по фишингу

Работу выполнил студент группы СКБ-213 _____ подпись, дата С. В. Патракеев

Работу выполнил студент группы СКБ-213 _____ подпись, дата Д. П. Коноваленко

Работу выполнил студент группы СКБ-213 _____ подпись, дата А. А. Альтамаре

Работу проверил _____ подпись, дата А. В. Сорокин

Москва 2023

Содержание

Общая идея эксперимента

Задача – провести дополнительные исследования на подверженность фишингу.

Предлагается три варианта сценария фишинговой атаки.

Первый вариант – текст письма будет опираться на недавнею утечку данных из НИУ ВШЭ. Человеку сообщается, что в связи с недавней атакой, в рамках устранения ущерба от нее, необходимо заполнить гугл форму и указать свои данные, которые могли бы находиться на серверах НИУ ВШЭ и оказаться в общем доступе, сделать это нужно как можно скорее. В тексте письма необходимо уверять пользователя, что перейти к гугл форме нужно как можно быстрее, так как от этого зависит безопасность и других его данных. Далее в письме идет гипертекст со ссылкой на ложную страницу входа в гугл аккаунт. Там пользователь может попытаться ввести свои данные и нажать кнопку «далее», после этого ничего не происходит. Будем считать количество переходов по ссылке, а так же количество нажатий кнопки «далее».

Второй вариант – в тексте письма предлагается пройти опрос по теме связанной, например с психологией. Опрос так же в формате гугл формы. Здесь можно ссылаться на то, что работу, для которой проводится опрос, необходимо сдать уже в ближайшие дни, и помощь каждого очень важна. В случае перехода по ссылке на опрос (так же гипертекст) сценарий сводится к первому случаю. Такой вариант подходит для соц. сетей, например беседа майнора по Психологии (около 400 человек) или же других подобных бесед, где часто распространяются опросы и т.п.

Третий вариант – текст письма опирается на 30-летие ВШЭ. Указывается, что в рамках улучшения качества обучения и работы сотрудников необходимо пройти опрос, также в гугл форме. Прохождение опроса необходимо и его важность приравнивается к СОП, со всеми вытекающими последствиями в случае игнорирования. Ссылка на опрос, представленная в виде гипертекста, так же, как и в предыдущих двух вариантах ведет на ложную страничку и далее сводится к 1 и 2 сценарию.

Заключение – из предложенных вариантов, можно выбрать два, например 1 и 2. 2 – для распространения в соц. сетях, а 1 – для почтовой рассылки. Использование в качестве канала распространения соц. сетей может дать возможность дополнительно оценить, насколько форма получения фишингового послания влияет на исход, так же средний возраст подопытных будет ниже, что позволит так же изучить влияние этого фактора. Более того, поскольку в беседе в соц. сетях собеседники могут сразу обмениваться информацией, можно будет понаблюдать, как быстро обнаружится, что ссылка является фишинговой и какая будет дальнейшая реакция.

Подготовка текста письма и оформление

Необходимо подготовить текст письма по выбранному сценарию и оформить его в соответствии с требованиями к общему стилю деловой рассылки. Для соц. сетей необходимо подготовить просто текст. При подготовке текста важно учитывать:

1. Должно быть минимальное количество ошибок, текст должен быть составлен грамотно и логично.
2. Необходимо соблюдать стиль в соответствие сценарию. Например, для соц. сетей текст не должен быть слишком сухим, нужно использовать разговорную лексику, сокращения и т.д.
3. Текст должен содержать посыл, который будет подгонять пользователя перейти по ссылке, как можно быстрее. Например, ссылать на важность опроса/письма, ограниченность времени и т.п.
4. Необходимо четко обозначить пользователю последствия при игнорировании письма и не переходе по ссылке. Последствия должны быть весомые, но при этом в рамках разумного. То есть за не прохождение опроса к 30-летию ВШЭ пользователя вряд ли отчислят, но возможно дисциплинарное предупреждение, как с СОП.

Подготовка технической части

Для проведения эксперимента необходимо подготовить:

1. Почтовые аккаунты для рассылки (3-4 штуки), почтовые аккаунты должны иметь имена связанные с сотрудниками/студентами НИУ ВШЭ. При отправке нескольких тестовых писем дошло именно то, где указывалось имя сотрудника ВШЭ и была соблюдена структура письма. Письмо в вольной форме без подписи сразу попало в Спам.
2. Аккаунты в соц. сетях (2-3 штуки) ВКонтакте и возможно Telegram. Там так же лучше использовать имена студентов, чтобы не вызывать подозрения раньше времени.
3. Отправить данные для входа в аккаунты в общую беседу проекта, чтобы упростить доступ программистам.

4. Копию страницы входа в аккаунт Google. Необходимо скопировать дизайн так, чтобы расхождения были минимальны. Проверить, что введенные данные нигде не сохраняются. Добавить функционал для подсчета количества переходов по ссылке. Добавить подсчет количества нажатий кнопки «Далее» (равносильно вводу данных).

Подготовка набора почтовых адресов для рассылки

Необходимо подготовить набор почтовых адресов для отправки фишинговых сообщений. В этот набор необходимо добавить как адреса сотрудников, так и студентов. Возможно провести отдельные рассылки для каждой из групп. Корпоративный почтовый адрес edu.hse.ru/hse.ru строится по принципе ПерваяБукваИмени_ПерваяБукваОчества_фамилия (svpatrakeev@edu.hse.ru – Сергей Владимирович Патракеев). Можно использовать этот шаблон и списки студентов в рейтингах/педагогический состав программы. Информацию можно брать с официального сайта. Процесс можно делать или вручную, или автоматизировать. Так же в интернете можно найти разные списки от поступивших, до участников тех или иных программ/мероприятий. Данные от туда так же можно использовать при составлении набора. Минимальный размер – 1000 адресов. Для соц. сетей достаточно выбрать несколько крупных бесед, где часто или, по крайней мере, иногда участники присылают свои опросы для работ, проектов.

Подготовка скрипта для рассылки

Для эффективного проведения эксперимента необходимо автоматизировать процесс отправки писем, желательно выдерживать некоторые интервалы между сообщениями. Для автоматизации процесса можно использовать язык программирования Python и модуль smtplib. Скрипт должен обеспечивать возможности:

1. Брать адреса из набора (csv/xlsx файл)
2. Выбрать аккаунт-отправитель
3. Указать тему письма
4. Отправлять письмо с указанным текстом по выбранным адресам
5. Выбирать интервал между сообщениями

Для удобства использования можно модифицировать скрипт как консольную утилиту с позиционными аргументами: путь до набора адресов, сколько адресов взять, путь до файла с настройками письма, интервал между сообщениями. В файл с настройками можно сохранять аккаунт-отправитель (почта, пароль для smtp), тему письма, текст сообщения.

Проведение эксперимента

После выполнения всех необходимых подготовительных действий, можно будет проводить сам эксперимент. Рассылку сообщений можно будет провести как в один день, так и в течение какого-то времени. Рассылку в соц. сетях лучше провести в другой день от почтовой, здесь лучше рассылать все в один день так как через какое-то время атака будет обнаружена и информация может начать распространятся среди студентов, снижая эффективность дальнейших атак. Более подробно спланировать эксперимент можно будет только после завершения всех подготовительных этапов.