УДК 159.99

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ: ПСИХОЛОГИЯ КИБЕРПРЕСТУПНИКОВ И МЕТОДЫ ЗАЩИТЫ

Можуго Д.В., студент гр. ИБт-231, II курс
Научный руководитель: Дементьева Ю.С., преподаватель
Кузбасский государственный технический университет
имени Т.Ф. Горбачева
г. Кемерово

В нашем мире, где технологии развиваются с быстрой скоростью, киберпреступность становится одной из самых серьёзных угроз для безопасности, как отдельных людей, так и организаций. Мы рассмотрим психологию киберпреступников, их методы и способы защиты от таких атак. Целью данной работы является раскрытие сути социальной инженерии и проведение опроса для выяснения, ознакомлено ли население с этой проблемой.

Для реализации цели были поставлены следующие задачи:

1. Определить понятие социальной инженерии.
2. Изучение видов атак с использованием социальной инженерии.
3. Проведение опроса среди населения.

Для выполнения работы были проведены следующие этапы, такие как: Сбор и анализ теоретических сведений, на котором были собраны и систематизированы данные. Так следующим этапом был проведён анализ информации, на основе которой были сформированы правила поведения, чтобы не попасться на уловки мошенника. Заключающим этапом стало проведение опроса и статистического анализа собранной информации.

Сформируем понятие социальной инженерии [1] – это способ манипуляции людьми при котором мошенник пытается, манипулируя психологией выкрасть конфиденциальные данные.

Для начала были обозначены виды преступлений с использованием социальной инженерии [2][3], чтобы на их основе научиться распознавать и предупреждать социальную инженерию в информационном пространстве.

Рассмотри виды атак с использованием социальной инженерии:

1. Ловля «на живца» - оставляет приманку в виде съемного носителя с вирусным ПО. А также есть такие устройства, которые способны повредить компьютеры, высвобождая мощный заряд через устройство.
2. Претекстинг — это вид мошенничества, когда злоумышленник с помощью заранее подготовленного выдуманного сценария пытается убедить жертву выдать секретную информацию или совершить определённое действие.
3. Фишинг — Вид мошенничества, при котором преступник пытается заполучить конфиденциальную информацию. А также есть целевой фи-

шинг — это фишинг при котором мошенники атакуют определённую группу лиц или одного человека, чтобы нанести урон определённой компании. Подтипами Фишинга являются: Вишинг (Фишинг — при котором вместо письма, мошенник звонит жертве) и Смишинг (Фишинг при котором вместо письма на электронную почту, используют SMS)

4. Незаконное получение доступа к вашей почте: Злоумышленник получает доступ к учетной записи жертвы, и к его контактам. После чего начинает рассылать последним фишинговые письма.
5. «Охота»: Преступник вступает в контакт с жертвой, начинает общаться, постепенно заставляя жертву доверять ему. После чего жертва сама начинает раскрывать некоторые конфиденциальные данные.
6. Тейлгейтинг — это вход злоумышленников в охраняемую зону вслед за уполномоченным лицом. Мошенник в таком случае выдаёт себя за представителя организации.
7. Вредоносные антивирусы — это программы, которые создают вирусные события, и сообщают о вредоносных программах, которых нет на вашем устройстве. Они собирают информацию о вас, а также предлагают купить полную версию, чтобы вылечить ваше устройство.
8. Фишинг по факсу — мошенник отправляет клиентам некоего банка запрос на подтверждение их конфиденциальных данных, с просьбой отправить по факсу на телефонный номер преступника.
9. Квид про кво — это преступление, когда вместо технического специалиста на запрос с решением проблемы с информационной системой отвечает преступник, выдавая свои действия за помощь с решением проблемы, в результате жертва сама совершает преступление.

Теперь же рассмотрим, как распознавать атаку, так для защиты важно в первую очередь проявлять рассудительность. Перед принятием решения следует его обдумать, и понять, перед вами реальный человек или правонарушитель. А следующие рекомендации помогут защитить людей от социальной инженерии:

Очень хорошо проверяйте адреса и профили в социальных сетях при получении странных сообщений. Зачастую мошенники подражают реально существующим людям. Благодаря чему люди, доверяющие своим друзьям, становятся жертвами.

Неверный синтаксис адреса сайта, плохое качество медиа материалов, старая или несуществующая в реальности символика компании, а также ошибки в словах должны заставить вас насторожиться. Такие признаки характерны для фишинговых сайтов.

Выгодные предложения – один из самых распространённых и действенных способов социальной инженерии. Преступники пытаются даже за незначительными на первый взгляд данными, например адресами электронной почты и номером телефона

Если собеседник не может подтвердить, что он действительно является представителем какой-то организации или компании, не делайте то, что он вам говорит. Это правило действует как в виртуальной, так и в живом мире

Теперь же рассмотрим, как предупредить атаки с использованием социальной инженерии:

- **Проверяйте источник**

Будьте осторожны с подозрительными сообщениями или объектами. Не используйте неопознанные внешние носители. Будьте осторожны с запросами на предоставление конфиденциальной информации. Всегда проверяйте источники информации.

- **Что им известно?**

Если человек, который вам звонит или пишет, не знает ваши данные, являющиеся персональными, но при это запрашивает их, это однозначно злоумышленник. Сотрудники компании, услугой которых вы пользуетесь, обычно имеют те данные, которые может обрабатывать.

Теперь составим краткие правила и рекомендации, которые помогут в защите от социальной инженерии. [4]

- Используйте надежный фильтр, он сможет отфильтровать нежелательный контент, будь то спам или фишинговое письмо.
- Оставайтесь бдительными при общении во всемирной паутине, ваш собеседник может оказаться преступником.
- Не позволяйте незнакомцам подключаться к вашей основной сети Wi-Fi, существуют программы, которые могут получить доступ через сеть.
- Устанавливайте обновления для всех приложений сразу после их выхода, несвоевременное поддержание базы данных, программ может оставить уязвимость.
- Для своих аккаунтов следует применять двухфакторную аутентификацию, она позволит лучше обезопасить ваши данные.
- Не работайте с важной информацией на глазах у посторонних людей, злоумышленник может подглядеть за вводом ваших данных.

Был проведён опрос об осведомленности среди преподавателей и студентов о том, что такое социальная инженерия и были ли среди них жертвы мошенников. Опрошено было более 100 человек.

По итогам опроса 1 (Рисунок 1) более 53,4% не знают, что такое социальная инженерия. Это плохой результат для учебного заведения, в планах предложение о проведении лекций о том, что такое социальная инженерия и как ей противодействовать. Так же, согласно опросу 2 (Рисунок 2) около 24,8% человек были жертвой мошенников и около 37,6% близких людей опрошенных были жертвами мошенников.

Рисунок 1 – Опрос 1

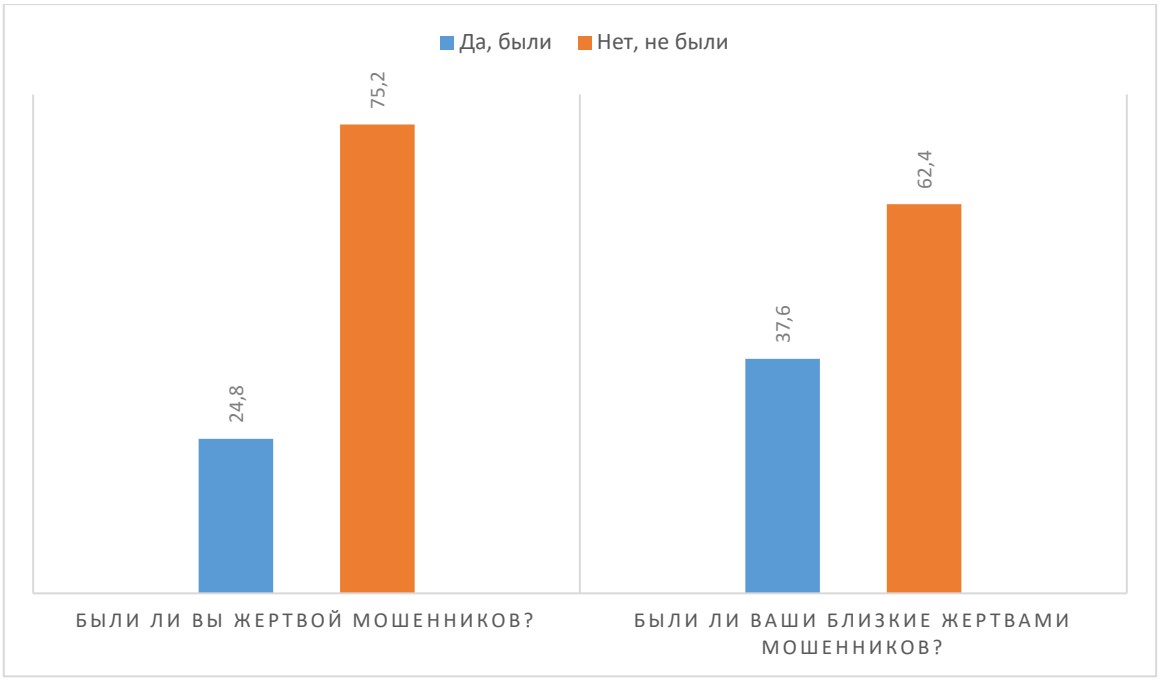

Рисунок 2 – Опрос 2

Список литературы:

1. Что такое социальная инженерия? Определение / [электронный ресурс] // kaspersky : [сайт]. – URL https://www.kaspersky.ru/resource-center/definitions/what-is-social-engineering
2. Социальная инженерия – защита и предотвращение / [электронный ресурс] // kaspersky : [сайт]. – URL https://www.kaspersky.ru/resource-center/threats/how-to-avoid-social-engineering-attacks

3. Что такое социальная инженерия и как противостоять атакам мошенников? / [электронный ресурс] // Центр кибербезопасности : [сайт]. – URL https://sec.ussc.ru/social_engineering
4. Что такое социальная инженерия: история, методы, примеры / [электронный ресурс] // рег.ру : [сайт]. – URL https://www.reg.ru/blog/chto-takoe-sotsialnaya-inzheneriya/?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru