**УДК 004.78**

# СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ КАК АСПЕКТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Наталия Владимировна Пчелинцева**
старший преподаватель
natas79@mail.ru
**Владислава Михайловна Ворошилова**
студент
VladaVM@yandex.ru
**Илья Валерьевич Чепраков**
студент
i.cheprakov@mail.ru
Мичуринский государственный аграрный университет
г. Мичуринск, Россия

**Аннотация.** В статье рассмотрено понятие социальной инженерии в контексте информационной безопасности, исследованы основные методы получения конфиденциальных данных при помощи социальной инженерии - рассылка фишинговых сообщений, распространение вредоносного программного обеспечения, спамов и др.

**Ключевые слова:** социальная инженерия, киберугрозы, информационная безопасность.

В кибербезопасности социальная инженерия - это искусство получения доступа к конфиденциальным данным путем манипулирования человеческой психологией, а не использования сложных методов взлома. Вместо того, чтобы использовать системную уязвимость, злоумышленник звонит сотруднику или отправляет фишинговое электронное письмо, выдавая себя за законный источник.

Как и другие киберугрозы, атаки социальной инженерии бывают различных форм. Понимание того, как они работают, - лучший способ снизить их риски. Существует несколько способов, которыми социальный инженер может использовать человеческую слабость.

Злоумышленник может обманом заставить вас оставить дверь открытой или загрузить вредоносный контент, который использует ваши сетевые ресурсы. Рассмотрим четыре шага социальной инженерии для успешной атаки.

Подготовка: на этом этапе социальные инженеры собирают информацию о своей цели. Социальные сети, звонки, электронная почта и текстовые сообщения - все это распространенные способы.

Проникновение: на этом этапе киберпреступники приближаются к своим целям, выдавая себя за законные источники, используя собранные данные о жертвах для аутентификации.

Эксплуатация: здесь злоумышленники манипулируют пользователями, чтобы раскрыть конфиденциальную информацию, такую как учетные данные для входа, данные учетной записи, контактную информацию, способы оплаты и многое другое, которые они могут использовать для выполнения своих атак.

Разъединение: на этом заключительном этапе социальный инженер прекращает общение с жертвой, проводит атаку и исчезает.

Время, необходимое для реализации такого плана, зависит от уровня атаки социальной инженерии — это может занять дни или даже месяцы. В любом случае, знание того, чего хотят социальные инженеры, и тактики, которые они используют, является отличным методом предотвращения социальной инженерии.

Социальные инженеры стремятся получить важную информацию, которую они могут использовать для кражи личных данных, получения финансовой выгоды или даже для подготовки к более целенаправленной атаке. Установка вредоносных программ для доступа к системам, учетным записям или личным данным является распространенной тактикой [1, 2].

Информация, которая является ценной для хакеров-социальных инженеров, включает в себя: номера учетных записей, данные для входа в систему, личная идентифицируемая информация, карточки доступа и удостоверения личности, информация о компьютерной системе, информация о сервере и сети.

Воздействие атак социальной инженерии на организацию может быть разрушительным. Это может запятнать её репутацию, нанести ущерб профессиональным отношениям и снизить доверие клиентов.

Кроме того, атаки социальной инженерии могут привести к серьезным финансовым потерям, сбоям в работе и снижению производительности бизнеса. Из-за этих потенциально катастрофических последствий для непрерывности бизнеса жизненно важно знать, как выявлять, предотвращать и противодействовать социальной инженерии. Внедрение надежной системы безопасности входящих и исходящих сообщений может помочь отслеживать трафик на предмет подозрительной активности пользователей, необычных доменов и электронных писем, а также массового перемещения конфиденциальных данных.

Существует несколько тактик манипулирования, которые социальные инженеры используют для достижения своих коварных целей. Выявление этих методов имеет решающее значение для предотвращения попадания вашей конфиденциальной информации в чужие руки. Рассмотрим некоторые тактики, используемые атакующими социальными инженерами.

Общение на эмоциональном уровне. Люди - эмоциональные существа, и они испытывают жалость, когда люди рассказывают трогательные истории.

Социальные инженеры часто создают истории или сценарии, чтобы убедить жертв раскрыть ценную информацию.

Используя рассуждения, которые могут вас обмануть: «Мне нужно войти в здание, потому что мне нужно встретиться с Джоном». На первый взгляд это звучит как веская причина, но стоит подумать о том, что это ничего не значит, если человека не пускают в здание, объяснение их встречи с Джоном является мошенническим. Однако слово «потому что» звучит так, будто причина веская.

Подарки и одолжения. Все любят подарки, и человеку свойственно стараться отвечать взаимностью на доброту. Злоумышленники могут использовать это для доступа к конфиденциальной информации или проникновения в офисное здание. Помните: бесплатные вещи - это всегда часть наживки.

Взаимность и симпатия. Социальные инженеры делают все, что в их силах, чтобы казаться симпатичными. Как только они обсудят этот аспект с жертвой, им будет намного легче заставить свою цель ответить взаимностью на их «доброту».

Целеустремленность и последовательность. Люди всегда хотят демонстрировать приверженность отношениям. Социальные инженеры могут воспользоваться этой человеческой природой, создавая небольшие обязательства. Даже упоминание вашего имени может быть воспринято как толчок к постоянству.

Авторитет и социальное доказательство. У каждого есть кто-то, на кого он равняется, многие люди в Интернете ищут чувство принадлежности. Как только киберпреступники распознают эти уязвимости, они могут использовать и то, и другое, чтобы утвердиться в глазах жертвы.

Дефицит и срочность. Социальные инженеры создают ощущение срочности, чтобы у жертв не было времени все обдумать. Если вы получили электронное письмо с просьбой выполнить срочное действие, лучше всего тщательно проанализировать ситуацию. Вы можете получить подтверждение от соответствующих органов, прежде чем выполнять какие-либо действия.

В зависимости от способа атаки доступно несколько тактик социальной инженерии. Чтобы избежать подобной атаки, организации должны понимать, что это такое и как она нацелена на них. Рассмотрим некоторые распространенные типы атак социальной инженерии

Фишинг. Это самая известная тактика социальной инженерии, используемая злоумышленниками. Злоумышленник создает поддельный портал поддержки или веб-сайт уважаемой компании и отправляет ссылки своим целям по электронной почте, чтобы обманом заставить их раскрыть конфиденциальную информацию.

Angler фишинг. Эта разновидность фишинга, нацеленного на аккаунты в социальных сетях. Злоумышленники подделывают учетные записи службы поддержки клиентов ведущих компаний, чтобы обмануть и убедить пользователей выдавать учетные данные для входа в систему и другие важные данные.

Шпионский фишинг. Это атака социальной инженерии, нацеленная на конкретные компании или отдельных лиц. Злоумышленник тратит дополнительное время на сбор информации о своей цели, чтобы сделать мошенничество подлинным. Конечная цель - украсть конфиденциальные данные.

Мошенничество с использованием китов или мошенничество с генеральным директором - это фишинговая атака, нацеленная на топ-менеджеров или высокопоставленных сотрудников компаний и государственных учреждений. Злоумышленник может подделать электронную почту генерального директора компании, а затем отправить письмо сотруднику с просьбой о срочном переводе или конфиденциальной информации.

Афера 419 / Нигерийский принц / Авансовый платеж - это тактика социальной инженерии, используемая злоумышленниками, чтобы обманом заставить жертв отправить авансовый платеж. В обмен злоумышленник обещает жертве крупную выплату или процент от средств.

Scareware. Это вредоносное программное обеспечение для обмана, которое заставляет пользователей компьютеров посещать зараженные веб-сайты. Атака может принимать форму рекламы или всплывающих окон от законных антивирусных компаний, сообщающих вам, что ваш компьютер заражен вирусом. Это пугает пользователей, заставляя их платить плату за решение проблемы безопасности.

Таббинг - это тактика социальной инженерии, которую злоумышленники используют для манипулирования неактивными веб-страницами. Это позволяет вредоносной веб-странице перенаправлять законный сайт на страницу злоумышленника. Как и другие тактики социальной инженерии, цель состоит в том, чтобы обманом заставить пользователей предоставить свои учетные данные.

Спам. Под спамом понимаются нежелательные сообщения, массово рассылаемые пользователям, как правило, в рекламных целях. Однако киберпреступники используют это для отправки сообщений, содержащих мошеннические ссылки, стимулы или предложения. Открытие такого электронного письма может заразить вашу систему или привести к загрузке программ-вымогателей на ваш компьютер.

Медовая ловушка - это тактика мошенничества, которая использует романтические или интимные отношения для личной или денежной выгоды. В большинстве случаев эта атака включает использование мошеннических сайтов знакомств для поиска жертв, кражи их денег и получения доступа к их конфиденциальной информации.

Компрометация деловой электронной почты. Данная фишинговая схема, при которой киберпреступники используют реальные или поддельные бизнес-аккаунты для обмана компании. Злоумышленник выдает себя за надежного источника, такого как генеральный директор, чтобы обманом заставить сотрудников совершать крупные переводы или предоставлять критически важные данные, которые они могут использовать для дальнейших атак.

Фарминг перенаправляет пользователей определенного веб-сайта на поддельную вредоносную версию. Цель состоит в том, чтобы заставить их предоставить учетные данные для входа [3].

Взлом электронной почты или перехват электронной почты - это киберугроза, используемая хакерами для получения несанкционированного доступа к учетным записям электронной почты. Цель состоит в том, чтобы украсть информацию для совершения мошенничества. Затем злоумышленники могут отправлять вредоносные электронные письма всем контактам. Обычно это отправная точка для олицетворения и захвата учетной записи.

Access tailgating. Это тактика, которую злоумышленники используют для доступа в здание или в закрытые зоны внутри здания. Злоумышленники используют различные способы для выполнения этой атаки, например, просят кого-то придержать дверь или используют предлог, чтобы получить доступ.

Наживка - это тактика, при которой мошенники обманом заставляют пользователей раскрывать личную и финансовую информацию в обмен на что-то взамен. Например, возможно получить электронное письмо с предложением подарочной карты в обмен на переход по ссылке для заполнения формы опроса.

Подмена DNS - это атака, которая изменяет запись доменного имени для перенаправления пользователей на мошеннический веб-сайт, похожий на предполагаемый адресат. Затем злоумышленник просит жертву войти в систему, давая им возможность украсть свои учетные данные.

Предлог - это атака социальной инженерии, которая обманом заставляет жертв разглашать конфиденциальные данные. Злоумышленник создает сфабрикованный или выдуманный сценарий, выдавая себя за законный или известный источник. В этой атаке злоумышленники могут физически получить доступ к вашим данным, выдавая себя за поставщика или курьера.

Физические нарушения связаны с физической кражей конфиденциальных документов и других ценностей, таких как накопители и компьютеры. Физические нарушения вызваны несанкционированным доступом в здание.

Атака через водопой - это киберугроза, при которой злоумышленник нацеливается на определенную группу пользователей, заражая сайт участников группы. Цель злоумышленника - заразить компьютеры жертв и получить доступ к критически важным сетевым ресурсам.

Услуга за услугу - это еще один метод социальной инженерии, при котором злоумышленники дают фальшивые обещания, чтобы заманить жертв в разглашение конфиденциальных данных. Например, возможен телефонный звонок человека, представляющегося представителем надежного поставщика услуг или службы ИТ-поддержки.

Диверсионная кража - это офлайн- и онлайн-кибератака, при которой злоумышленники перехватывают поставки и перенаправляют их в неправильное место. Мошенники также используют эту тактику, чтобы заманить жертв в раскрытие конфиденциальной информации.

Очень важно расставить приоритеты в методах предотвращения социальной инженерии в качестве основного компонента плана кибербезопасности. Организации должны применять целостный подход, который сочетает в себе сложные инструменты безопасности, протоколы и регулярные тренинги по кибербезопасности для персонала и руководителей. Рассмотрим меры, которые можно реализовать для противодействия рискам социальной инженерии.

Политики и протоколы безопасности должны быть неотъемлемой частью плана кибербезопасности. Эти меры расскажут сотрудникам, как безопасно получать доступ к ресурсам организации, таким как электронная почта, мобильные устройства и пароли, и обращаться с ними. Рассмотрим некоторые аспекты, которые стоит рассмотреть.

Политики и протоколы безопасности организации должны обеспечивать двухфакторную и многофакторную аутентификацию. Это повышает безопасность организации, поскольку сотрудникам предлагается входить в систему не только под своим именем пользователя и паролем. С помощью 2FA или MFA злоумышленники-социальные инженеры по-прежнему не могут

получить доступ к учетным записям вашей компании, даже если у них есть данные для входа.

Частая смена пароля и хорошая гигиена пароля. Соблюдение правил гигиены паролей должно быть обязательным. Следует поручить сотрудникам часто менять свои пароли, следует использовать надежный пароль, который хакерам трудно угадать. Надежный пароль включает в себя как прописные, так и строчные буквы, цифры и специальные символы. Кроме того, необходимы разные пароли для разных учетных записей [4, 5].

Регулярное тестирование атак на проникновение является ключом к общей защите безопасности. Это позволяет находить пробелы в процедуре безопасности. Можно смоделировать реальную атаку, чтобы проверить сотрудников и сеть на наличие уязвимостей. Благодаря этому возможно использовать упреждающий подход для оценки и постоянного улучшения своей сети ИТ-инфраструктуры.

Социальная инженерия использует человеческие ошибки для компрометации сетей. Поэтому важно включить сотрудников в план обеспечения безопасности. Они являются первой линией обороны. Обучение защите в области социальной инженерии должно снабдить членов организации соответствующими инструментами для выявления киберугроз, самозащиты и защиты организации.

Правильное управление мобильными устройствами является еще одним важным компонентом эффективных профилактических мер социальной инженерии. Сотрудники, использующие мобильные устройства компании, должны использовать надежные пароли и устанавливать современное антивирусное программное обеспечение.

Внедрите строгие правила BYOD (принесите свое устройство), регулирующие, как сотрудники используют свои устройства в офисе или при работе из дома.

Организации, которые полагаются на сторонних поставщиков, могут понести репутационный ущерб в результате нарушений со стороны третьих

лиц. Даже если это не является нормативным требованием, организации должны включать в свой план обеспечения безопасности план управления сторонними организациями. Он обеспечивает ценный контроль и информацию о снижении рисков, возникающих в результате этих внешних деловых отношений [5].

Утечки данных раскрывают конфиденциальную информацию, такую как данные для входа, данные кредитной карты и адреса электронной почты. Социальные инженеры могут приобретать эту информацию из темной сети для попыток фишинга или других атак по электронной почте. По этой причине организациям следует внедрить решение для предотвращения потери данных (DLP), чтобы предотвратить утечку конфиденциальных данных с конечных устройств.

Социальная инженерия является одним из наиболее распространенных видов кибератак, угрожающих безопасности корпораций. Организации и сотрудники должны понимать негативные последствия успешных кибератак. Это может привести не только к потере данных, но и к более серьезным последствиям, таким как финансовые потери и даже ущерб непрерывности бизнеса.

Понимание того, как работают социальные инженеры и чего они хотят, является первым шагом к предотвращению вредоносных атак. План кибербезопасности должен включать регулярное тестирование на проникновение и управление рисками сторонних организаций, а также ведение строгих правил политики безопасности и обучение сотрудников методам социальной инженерии для предотвращения этих атак.

**Список литературы:**

1. Павлова Ю. В., Быкова А. В. Социальная инженерия: основные методы воздействия социальных хакеров // Молодая экономическая наука: материалы 63-й научной конференции студентов и магистрантов по экономическим наукам. Самара. 25–27 апреля 2008 года. Самара. 2009. С. 94-99.

2. Дьяков Н. В. Применение методов социальной инженерии в социальных сетях // Общество. 2020. № 2(17). С. 126-128. – EDN IGGPSP.

3. Ярославцева К.А., Пчелинцева Н.В., Чепраков И.В., Картечина Н.В. Этические проблемы цифровых технологий// В сборнике: Инженерное обеспечение инновационных технологий в АПК. Материалы Международной научно-практической конференции. Под общей редакцией И.П. Криволапова. Мичуринск-наукоград. 2022. С. 255-258.

4. Чепраков И. В., Пчелинцева Н.В., Гущина А.А. Искусственный интеллект, его проблемы и перспективы // Наука и Образование. 2022. Т. 5. № 2.

5. Гущина А.А., Пчелинцева Н.В., Шацкий В.А. Применение искусственного интеллекта в обеспечении безопасности данных //В сборнике: Инженерное обеспечение инновационных технологий в АПК. Материалы Международной научно-практической конференции. Мичуринск-наукоград РФ. 2021. С. 79-81.

**UDC 004.78**

## SOCIAL ENGINEERING AS AN ASPECT OF INFORMATION SECURITY

**Natalia V. Pchelintseva**
senior lecturer
natas79@mail.ru

**Vladislava M. Voroshilova**
student
VladaVM@yandex.ru
**Ilya V. Cheprakov**
student
i.cheprakov@mail.ru
Michurinsk State Agrarian University
Michurinsk, Russia

**Annotation.** The article examines the concept of social engineering in the context of information security, examines the main methods of obtaining confidential data using social engineering - phishing messages, distribution of malicious software, spam, etc.

**Keywords:** social engineering, cyber threats, information security.

Статья поступила в редакцию 16.02.2023; одобрена после рецензирования 20.03.2022; принята к публикации 30.03.2023.

The article was submitted 16.02.2023; approved after reviewing 20.03.2022; accepted for publication 30.03.2023.