Доверие и безопасность в информационном обществе

ПОДХОДЫ К КЛАССИФИКАЦИИ СОЦИОИНЖЕНЕРНЫХ АТАК

Статья рекомендована к публикации членом редакционного совета А. А. Стрельцовым 25.10.2024.

Тулупьева Татьяна Валентиновна

Кандидат психологических наук, доцент
Российская академия народного хозяйства и государственной службы при Президенте РФ (РАНХиГС), референтура, советник проректора
Москва, Российская Федерация
Санкт-Петербургский федеральный исследовательский центр Российской академии наук, лаборатория прикладного искусственного интеллекта, старший научный сотрудник
Санкт-Петербург, Российская Федерация
tulupeva-tv@ranepa.ru

Абрамов Максим Викторович

Кандидат технических наук, доцент
Санкт-Петербургский федеральный исследовательский центр Российской академии наук, руководитель лаборатории прикладного искусственного интеллекта
Санкт-Петербург, Российская Федерация
mva@dscs.pro

Азаров Артур Александрович

Кандидат технических наук
Российская академия народного хозяйства и государственной службы при Президенте РФ (РАНХиГС), проректор по науке
Москва, Российская Федерация
azarov-aa@ranepa.ru

Аннотация

Целью данной статьи является разработка классификации социоинженерных атак, учитывающей специфику атаки и ее этапы для дальнейшего построения моделей оценки защищенности пользователей от таких атак. Изучение имеющихся в литературе подходов к классификации социоинженерных атак позволило охватить выделяемые виды атак и выявить пересечения и пробелы в имеющихся классификациях. Разработанный подход к классификации позволяет выделить разнообразные виды атак, учитывающие поэтапность и сложность воздействия. Введение претекстинга на этапе подготовки позволяет выделять целевые и нецелевые атаки, которые в сочетании с выбранными средствами контакта с жертвой дают диапазон различных видов атаки. Представленная классификация социоинженерных атак создает основу для построения вероятностных моделей оценки защищенности пользователей, успеха реализации атаки. Подходы, основанные на более ранней версии классификации, не позволяли в высокой степени полноты агрегировать необходимые параметры, влияющие на успешность атаки. Избранный подход к классификации, ассоциированный с этапами атаки, позволяет моделировать процесс и прогнозировать его результаты. Результаты данного исследования будут интересны специалистам в области управления персоналом, подготовки кадров, информационной безопасности, информационных технологий, искусственного интеллекта; руководителям, владельцам бизнеса, руководителям государственных и муниципальных органов.

Ключевые слова

информационная безопасность, социальное влияние, фишинг, претекстинг, социоинженерные атаки

https://doi.org/10.52605/16059921_2025_03_103

Введение

Обеспечение информационной безопасности как частных лиц, так и организаций всё чаще становится ключевым фактором стабильности развития современного общества. И если всего лишь 5–10 лет назад интернет-сообщество будоражили новости о взломе тех или иных серверов банков, министерств и ведомств, то теперь фокус внимания существенным образом сместился на нарушения, связанные с кражей имущества частных лиц. Немаловажным фактором, влияющим на взрывной рост киберпреступлений, является развитие современных технологий, позволяющих моделировать голос и изображение человека, изменять документы, подделывать чаты. Злоумышленники успешно мимикрируют под известных и доверенных лиц жертвы, что значительно повышает шансы таких киберпреступлений. Всё это приводит как к ярким хищениям, в которых фигурируют десятки миллионов рублей, так и к постоянным, ежедневным злодеяниям, жертвами которых становятся обычные граждане. По данным МВД, в 2023 году количество преступлений в сфере информационно-телекоммуникационных технологий увеличилось на 29,7% по сравнению с предыдущим годом. Их доля в общем числе преступных деяний возросла до 34,8%. Также увеличилось количество дистанционных мошенничеств и краж (70,2%). Раскрытие киберпреступлений остаётся на низком уровне — 25,5. В связи с этим изучение факторов, определяющих степень доверия людей к цифровым технологиям, а также умение распознавать социоинженерные атаки становится особенно актуальным на сегодняшний день.

Большинство такого рода преступлений построено на методах социоинженерного воздействия на человека. Благодаря применению ряда манипулятивных технологий перед жертвой разворачивается настоящее представление, с предъявлением подложных документов, постоянным вовлечением в переговоры с различными, якобы, должностными лицами. Существуют сценарии проведения такого рода социоинженерных атак, в случае успеха которых итогом становится потеря человеком существенных финансовых средств и/или репутационные издержки.

Таким образом, социоинженерные атаки крайне эффективны в условиях настоящего развития технологий и требуют повышенного внимания от организаций для митигации соответствующих рисков. Существуют разные подходы к защите пользователей от социоинженерных атак, но для их эффективного внедрения требуется анализ текущей ситуации. Анализ защищенности пользователей информационных систем от социоинженерных атак можно производить через пентесты, когда нанимается компания, которая имитирует социоинженерную атаку и выявляет сотрудников, которые способствовали успеху атаки. Но такой способ не всегда оправдан с точки зрения эффективности сотрудников и их лояльности к компании. Можно выявлять риски через коммуникацию с сотрудниками, но этот способ очень ресурсозатратен. Другая группа подходов, разрабатываемая в том числе коллективом авторов статьи [Азаров и др., 2016], основана на анализе защищенности пользователей от социоинженерных атак через выявление уязвимостей пользователей и их связей с личностными особенностями. Оценку выраженности личностных особенностей можно проводить через анализ цифровых следов пользователей. Такие подходы для построения соответствующих моделей требуют классификации социоинженерных атак, которая позволила бы связать классы атак с личностными профилями пользователей, наиболее им подверженных. Построение таких моделей с более точными, чем ранее, оценками позволило бы принимать комплексные превентивные меры, снижающие риски реализации социоинженерных атак и соответственно нивелирующие ущерб. Резюмируя, мы имеем противоречие, с одной стороны востребованности новой классификации, с другой стороны отсутствия ее в научной литературе. В связи с чем актуальной видится задача, решаемая в статье, по построению классификации социоинженерных атак.

1 Социоинженерные атаки

Под социоинженерной атакой будем понимать совокупность действий злоумышленника, направленных на другое лицо (или группу лиц) с целью достижения желаемого результата, в частности, нарушения безопасности информации [Азаров и др., 2016]. Социоинженерная атака является разновидностью акта социального влияния. Если использовать обобщенное определение социального влияния [Тулупьева и др., 2021], то под ним подразумевается воздействие на аффективную, когнитивную или поведенческую сферу человека с целью получить изменения в этих сферах. Если говорить в контексте социоинженерных атак, то этой целью является изменения в поведенческой сфере, к ним можно отнести совершение определенных действий, ведущих к

компрометации данных, а изменения в аффективной и когнитивных сферах являются лишь частью атаки, подготовкой для изменения поведения.

Интегральная модель социального влияния [Тулупьева и др., 2021], разработанная авторами, легла в основу модели социоинженерной атаки, в которой злоумышленник выступает в роли агента влияния, а пользователь информационной системы или держатель нужной информации, с которым можно вступить в контакт посредством технических средств, — в роли реципиента. Чем больше у злоумышленника во владении доступных ресурсов (входящие в модель самого злоумышленника) [Abramov, Tulupyev, 2019; Тулупьева, 2022], тем успешнее окажется социоинженерная атака. При правильном подборе способов влияния и технических средств для контакта с жертвой злоумышленник с большей вероятностью достигает своей цели – вынудить жертву совершить действие, которое предоставит злоумышленнику доступ к желаемой информации или активу. Примером таких атак являются звонки мошенников из, якобы, службы безопасности банка или отделения полиции с требованием перевести деньги на «безопасные» счета, чтобы сохранить их.

Социоинженерные атаки в киберпространстве по своей механике похожи на социальное воздействие в реальном мире, но наблюдается ряд отличий. Интернет пространство предоставляет злоумышленнику больше возможностей для персонализации атак, поскольку, пользователи представляют о себе много информации в открытом доступе. Возможная анонимность цифровых каналов позволяет злоумышленнику защитить свою личность, что, как ему кажется, может помочь избежать юридических проблем, связанных с его действиями. Кроме того, цифровые каналы также позволяют злоумышленнику проводить одновременные веерные атаки на жертв, снижая затраты на проведение социоинженерных атак и увеличивая шансы найти жертву из-за эффекта масштаба. Задача потенциальной жертвы, чтобы защитить себя от негативных последствий, — выявить социоинженерные атаки, избегая при этом высокого уровня ложноположительных результатов.

2 Виды социоинженерных атак

К настоящему моменту рядом авторов было предпринято несколько попыток создать классификацию социоинженерных атак, но анализ имеющихся классификаций показал, что в них часто встречается пересечение классов, во многих не выделено основание для классификации, а содержится просто перечисление видов атак. Анализ подходов показал, что имеются следующие основания для классификации.

Первое основание для классификации – непосредственное участие человека в социоинженерной атаке, в контакте с жертвой. При таком основании выделяются две категории: с участием человека и без непосредственного участия человека, с помощью технического средства [Xiangyu, et al., 2017]. Встречается и другое название этих классов атак: прямые и косвенные [Salahdine, Kaabouch, 2019]. При атаках с участием человека злоумышленник осуществляет атаку лично, взаимодействуя с целью для сбора необходимой информации. Поскольку временные резервы человека ограничены и в каждый конкретный момент времени злоумышленник может общаться с одной жертвой, то при таком типе атак он может повлиять на небольшое число жертв. Программные атаки, осуществляемые с использованием таких устройств, как компьютеры или мобильные телефоны, могут атаковать множество жертв за несколько секунд. Такие массовые рассылки являются разновидностью массового фишинга [Koyun, Aljanaby, 2017]. В этом смысле для манипуляции можно выделить и другую форму взаимодействия — размещение фейковой, но привлекательной информации на веб-сайте или в социальных сетях. Здесь количество потенциальных целей может быть очень большим, даже если ложная информация публикуется с целью привлечь внимание конкретных групп.

Второе основание для классификации базируется на способах проведения атаки: социальные, технические и физические атаки [Kalnin, et al., 2017]. Атаки на социальной основе осуществляются через использование психологических свойств и эмоциональных состояний жертвы. Правильнее их было бы назвать социально-психологическими. Эти атаки считаются наиболее чувствительными для жертвы, поскольку они предполагают взаимодействие людей [Patil, Devale, 2016]. Примерами таких атак являются претекстинг (придумывание фальшивых, но убедительных для жертвы сценариев, основанных на фактах из ее жизни, с целью получения нужной личной информации и повышения уровня доверия жертвы) и целевой фишинг (социоинженерная атака на конкретную жертву с опорой на ее профиль уязвимости). Атаки технического характера проводятся через

Интернет через социальные сети и веб-сайты онлайн-сервисов и собирают необходимую информацию, такую как пароли, данные кредитной карты и контрольные вопросы [Kalnin, et al., 2017]. Физические атаки — это действия в реальном пространстве, выполняемые злоумышленником для сбора информации о цели. Примером таких атак является поиск ценных документов в мусорных контейнерах, физический доступ, серфинг (подглядывание) через плечо и кража важных документов [Pokrovskaia, 2017]. Такие атаки не будут рассматриваться в рамках данной статьи.

Перейдем к описанию самих видов социоинженерных атак. Наиболее распространенными являются фишинговые атаки [Chiew, et al., 2018; Gupta, et al., 2016; Yeboah-Boateng, Amanor, 2014]. Их цель — обманным путем получить желаемую целевую информацию от намеченных жертв посредством телефонных звонков, смс или электронных писем. Например, атакой может быть звонок или электронное письмо из поддельного отдела лотереи о выигрыше денежной суммы, прекращении обслуживания телефонного номера, необходимости пройти диспансеризацию и запросе личной информации или переходе по ссылке, прикрепленной к электронному письму. Этими данными могут быть данные банковской карты, паспортные данные, полное имя, домашний адрес, имя домашнего животного, девичья фамилия матери, место рождения, место учебы или любая другая информация, например, ответы на частые секретные вопросы, которую человек может использовать для входа в учетные записи, такие как как онлайн-банкинг или услуги [Peotta, et al., 2011].

Koyun, A.; Aljanaby, E. делят фишинговые атаки на семь категорий: фишинг-рассылка, целевой фишинг, китобойный фишинг, вишинг-фишинг, фишинг с интерактивным голосовым ответом, смс-фишинг или смишинг и фишинг с компрометацией деловой электронной почты [Koyun, Aljanaby, 2017].

Нецелевой фишинг или рассылка — это мошенническая практика отправки электронных писем или сообщений на несколько адресов сразу, обычно исходящих из известного источника (важной организации) с целью кражи конфиденциальной информации, такой как пароли, номера кредитных карт и т. д.

Целевой фишинг — это фишинг, направленный на конкретных лиц или отдельные группы. Для этого вида атак нужно собрать информацию о жертве, используя доступные данные в Интернете [Ho, et al., 2017]. Злоумышленники изучают поведение своих целей и собирают информацию, чтобы сделать атаку правдоподобной и повысить вероятность ее успеха.

Китобойный фишинг — это направленная фишинговая атака, нацеленная на высокопоставленных лиц в компаниях, называемых «крупными рыбами». В этой форме фишинга основной характеристикой является тип цели, представленный высшими руководителями, представителями государственных учреждений, политиками и знаменитостями. Учитывая актуальность цели (крупная рыба), ценность информации особенно привлекательна для киберпреступников. Как и целевой фишинг, мошенническое электронное письмо создается специально и похоже, что оно исходит от делового партнера [Corradini, 2020].

Фишинг с компрометацией деловой электронной почты имитирует китобойный промысел, нацеленный на крупных «рыб» в корпоративном бизнесе, чтобы получить доступ к их деловой электронной почте, календарю, платежам, бухгалтерскому учету или другой личной информации [Opazo, et al., 2018]. Злоумышленник начинает с исследования высокопоставленных сотрудников через социальные сети, чтобы узнать и понять их профессиональную информацию [Wilcox, Bhattacharya, 2016]. Получив нужную информацию, злоумышленник отправляет весьма убедительное деловое электронное письмо, чтобы заставить обычного сотрудника щелкнуть ссылку или загрузить вложение к электронному письму, чтобы скомпрометировать сеть компании. Злоумышленник может создать фейковый аккаунт, с которого рассылает сообщения сотрудникам и подчиненным, может выдавать себя за руководителя организации, чтобы заставить уполномоченного сотрудника этой организации выполнить банковский перевод на счет, контролируемый тем же злоумышленником. Такой вид атаки очень распространен в последние несколько месяцев.

Вишинговые атаки относятся к телефонному фишингу с целью манипулирования людьми, чтобы они предоставили свою конфиденциальную информацию для проверки, например, звонки из банка [Yeboah-Boateng, Amanor, 2014]. Название этой атаки, «вишинг», происходит от слова «голос» и «фишинг» для описания атак, выполняемых через голосовую связь [Hofbauer, et al., 2015]. Здесь, учитывая, что мошеннические действия совершаются по телефону, для успеха атаки

необходимы сочувствие и умение вести разговор. Фишинг с интерактивным голосовым ответом осуществляется с использованием системы интерактивного голосового ответа, которая заставляет цель вводить личную информацию, как если бы она исходила от законного бизнеса или банка [Braun, et al., 2018].

СМС-фишинг (Смишинг) — тип атаки с использованием мобильных телефонов могут осуществляться посредством служб коротких сообщений (SMS) или текстовых сообщений, которые известны как атаки SMSishing [Ivaturi, Janczewski, 2011]. СМС-атаки заключаются в отправке жертвам мошеннических сообщений через мобильные телефоны с целью повлиять на них. Полученное текстовое сообщение может содержать вредоносное ПО, даже если оно было отправлено от надежного и известного передатчика.

Анализ описанных классификаций показывает, что в них есть пересечения. Например, смс-фишинг является просто разновидностью фишинга и может быть как массовым, так и целевым. Выделение целевого фишинга приводит к необходимости добавлять в классификацию претекстинг.

Претекстовые атаки заключаются в придумывании фальшивых и убедительных сценариев с целью кражи личной информации жертвы. Они основаны на предлогах, которые заставляют жертву поверить и довериться нападавшему. Претекстинг состоит, например, в выдаче себя за кого-то другого, т.е. полицейский или страховой следователь. Атака осуществляется посредством телефонных звонков, электронной почты или физических носителей. Предлогом может быть предложение оказать услугу или устроиться на работу, вопрос о личной информации, помощь другу в получении доступа к чему-либо или выигрыш в лотерею.

Для повышения успешности социоинженерной атаки используют приманку. Некоторые авторы выделяют приманку в отдельный вид социоинженерной атаки [Krombholz, et al., 2014]. На самом деле приманка является составной ее частью. Мы предлагаем рассматривать приманку в широком смысле, не только обещание какого-то вознаграждения, но и угроза является приманкой.

Ряд авторов [Wang, et al., 2018; Kim, et al, 2017] пишут о программах-вымогателях как виде социоинженерных атак. Но для того, чтобы программа-вымогатель сработала, она должна попасть в систему. А значит, она не может расцениваться как самостоятельная социоинженерная атака, а лишь как часть ее. Таким же образом можно расценивать и поддельные сайты [De Ryck, et al., 2013]. Злоумышленник использует доверие жертв к этим веб-сайтам и получает доступ к их учетной информации [Suri, et al., 2012].

Deepfake — это недавняя техника, используемая для проведения социоинженерных атак. Киберпреступники используют дипфейки для подделки изображений, аудио и видео для достижения определенной цели. В сфере кибербезопасности дипфейки представляют собой растущую угрозу [Albahar, Almalki, 2019; Chi, et al., 2020].

3 Классификация социоинженерных атак

Для построения классификации, охватывающей имеющиеся виды, целесообразно привязать ее к этапам социоинженерной атаки. Среди типичных этапов СИА выделяют [Algarni, et al., 2013; Тулупьева, 2022]:

1) Сбор информации об организации и жертве;

2) Развитие отношений с жертвой (выбор канала установления контакта и контакт с жертвой);

3) Эксплуатация отношений (предъявление приманки в виде вознаграждения или угрозы);

4) Исполнение, направленное на достижение цели (совершение жертвой вредоносного для нее действия).

Этап 1 подразумевает претекстинг, если запланирована целевая социоинженерная атака и нахождение данных для массового доступа, если атака нецелевая.

На этапе 2 можно выделить несколько типов атак по установлению контакта с жертвой. К ним можно отнести: мейл-фишинг (контакт по электронной почте), мессенджеровый фишинг (контакт через мессенджеры), вишинг (контакт через голосовую связь), смишинг (контакт через смс), социальные сети (поддельный профиль в социальных сетях, включая сайты знакомств), веб-сайт (поддельные сайты и сайты-маски)

Отсутствие претекстинга подразумевает реализацию массовых контактов с жертвами через все эти типы атак, включая голосовую связь. В случае с голосовой связью происходит автоматизированный голосовой контакт с заранее заданным скриптом, который может быть достаточно сложным и разветвленным.

Наличие претекстинга позволяет осуществить целевую атаку по трем типам: от неизвестного отправителя (в этом случае нужны дополнительные меры по формированию доверия к этому отправителю), от известной организации (примером являются звонки от службы безопасности банков, звонки или сообщения от операторов мобильной связи или из поликлиник с требованием пройти флюорографию) и от известного жертве авторитетного лица (примером являются сообщения по почте или в мессенджерах от руководителя, что с жертвой будет связываться, например, заместитель министра). Совсем недавно прошла информация об усложненной схеме целевой атаки, при которой жертва получает письмо с сообщением о входе в кабинет адресата на «Госуслугах» с нового устройства и с требованием позвонить по указанному номеру. В процессе звонка у жертвы выясняют реальные сведения для входа в аккаунт[1].

На этапе 3 можно выделить два типа атак: атака-поощрение или атака-угроза. Примерами первого типа могут быть атаки с обещанием удвоения пополнения счета мобильного телефона, если его пополнить, пройдя по ссылке. К этому же типу относятся широко описываемые в сети интернет «медовые ловушки», которые часто используются на сайте знакомств. Состоит она в создании злоумышленником поддельного профиля привлекательного человека, чтобы заманить жертву и выведать у нее нужную информацию или получить деньги. Чаще всего «медовая ловушка» является массовой атакой, когда злоумышленник ставит лайки большому числу потенциальных жертв, а потом развивает отношения с ними в процессе диалога.

На этапе 4 выделяются разные виды действий, которые могут привести утечке данных: к ним относятся сообщение своих персональных данных в явном виде, переход по ссылке, установка на электронное устройство вредоносной программы, выход на поддельный сайт.

Основываясь на описанных типах, классификацию социоинженерных атак можно представить следующим образом (Рис. 1).

Опираясь на эту классификацию, удобно выстраивать различные виды атакующего воздействия. Например, нецелевая рассылка по электронной почте с обещанием вознаграждения при переходе по ссылке с введением персональных данных; целевой контакт в мессенджере от имени руководителя организации с угрозой потери финансовых средств и требованием раскрыть данные (поступивший код для входа); целевой контакт по голосовой связи от известного банка с угрозой блокировки счета и требованием установить программу из присланной СМС. Данная классификация позволяет предусмотреть большое множество атак, построить их траектории и предусмотреть меры профилактики на каждом этапе. Важным превентивным моментом является распространение информации о многочисленных видах атак для широкой аудитории, чтобы любой пользователь информационной системы имел возможность распознать воздействие, которое на него пытаются оказать злоумышленники

[1] https://finance.mail.ru/2024-08-24/ne-zvoni-im-ne-zvoni-moshenniki-pridumali-shemu-s-netipichnym-vhodom-v-gosuslugi-62495757/?fromnews=1&frommail=1 (доступ 24.08.2024)

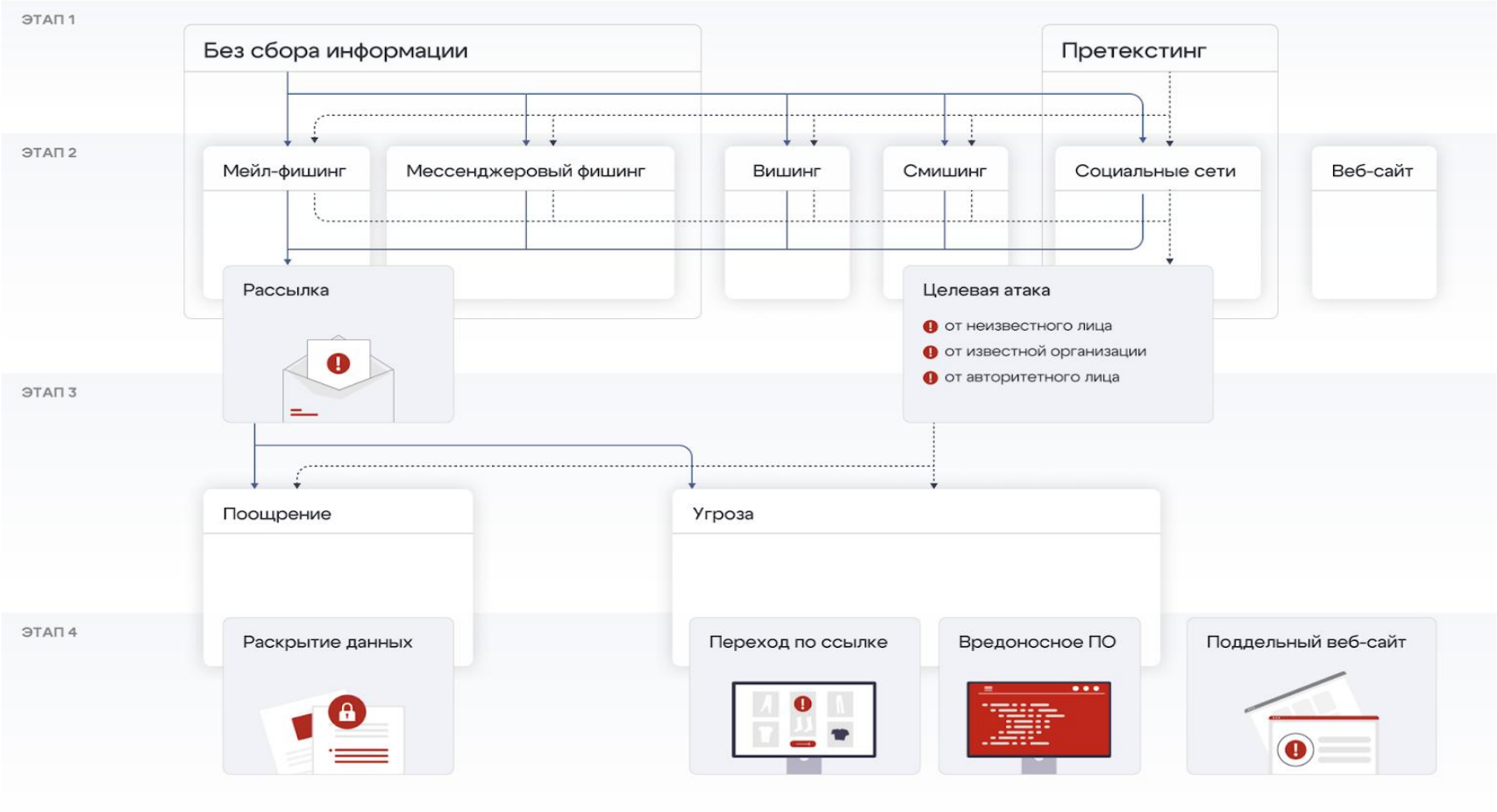

Рис. 1. Классификация социоинженерных атак

Модели

Для анализа применимости представленного подхода представляется целесообразным рассмотреть следующую совокупность моделей, применимых для оценки защищенности пользователей информационных систем организаций. С незначительными изменениями данные модели могут быть использованы и для отражения взаимодействия частных лиц и злоумышленников. Совокупность моделей и подходов к оценке защищенности пользователей была более подробно описана в [Азаров и др., 2016; Абрамов М.В. и др., 2018]

Если рассмотреть общие алгебраические модели для представления параметров, которые должны учитываться при построении оценок защищённости пользователей информационных систем от социоинженерных атак и оценок вероятности поражения критичных документов, то можно построить модели оценок, представленные ниже. Пусть модель критичных документов содержит компоненты, которые связаны с уровнем критичности для компании, расположением на хостах и доступом к документу с них, уровнем доступа пользователей к документу и иные [Абрамов М.В. и др., 2018]. Пусть модель пользователя информационной системы формализована как $U_i = \left(\left\{ \left(V_j, D_i(V_j) \right) \right\}_{j=1}^{n}; \left\{ \left(\mathrm{AH}_l^i; \mathrm{LAH}_l^i \right) \right\}_{l=1}^{m}; \left\{ \left(\mathrm{AD}_k^i; \mathrm{LAD}_k^i \right) \right\}_{k=1}^{q}; \left\{ \mathrm{Comm}_t^i \right\}_{t=1}^{r}; \left\{ \mathrm{CA}_a^i \right\}_{a=1}^{b}; \mathrm{State}_g^i \right)$, где $\left\{ \left(V_j, D_i(V_j) \right) \right\}_{j=1}^{m}$ — профиль уязвимостей пользователя, в котором V_j — уязвимость, а $D_i(V_j)$ — выраженность V_j, $\left\{ \left(\mathrm{AH}_l^i; \mathrm{LAH}_l^i \right) \right\}_{l=1}^{m}$ — хосты с уровнем доступа к ним, $\left\{ \left(\mathrm{AD}_k^i; \mathrm{LAD}_k^i \right) \right\}_{k=1}^{q}$ — документы с уровнем доступа к ним, $\left\{ \mathrm{Comm}_t^i \right\}_{t=1}^{r}$ — тип взаимоотношений пользователя с другими пользователями информационной системы, $\left\{ \mathrm{CA}_a^i \right\}_{a=1}^{b}$ — контролируемые зоны, доступные ему, State_g^i — внутреннее состояние, которое может влиять на его ответные действия при атаке.

Формализация модели злоумышленника может быть представлена следующим образом $M_i = \left(\left\{ \left(R_j, Q_i(R_j) \right) \right\}_{j=1}^{n}; \left\{ \left(A_k, S_i(A_k) \right) \right\}_{k=1}^{m}; \left\{ \mathrm{BK}_l^i \right\}_{l=1}^{q}; G^i; \left\{ \mathrm{Comm}_t^i \right\}_{t=1}^{r} \right)$, где $\left\{ \left(R_j, Q_i(R_j) \right) \right\}_{j=1}^{n}$ — ресурсы, доступные злоумышленнику (например, время, деньги или личностные особенности злоумышленника), $\left\{ \left(A_k, S_i(A_k) \right) \right\}_{k=1}^{m}$ — профиль компетенций злоумышленника (компетенция злоумышленника и степень умения использовать им определённое атакующее действие рассматриваются как синонимы), $\left\{ \mathrm{BK}_i \right\}_{i=1}^{l}$ — начальные знания злоумышленника об архитектуре системы (её сотрудниках, их уязвимостях, доступных им критичных документах, взаимоотношениях персонала и контролируемых зонах), G^i — цель злоумышленника, $\left\{ \mathrm{Comm}_t^i \right\}_{t=1}^{r}$ — связи злоумышленника с другими злоумышленниками.

Профиль компетенций злоумышленника может быть охарактеризован степенью умения злоумышленника использовать определённые типы социоинженерных атакующих воздействий. Формализация профиля компетенций злоумышленника может быть представлена в виде $((A_1, S(A_1)), \ldots, (A_q, S(A_q)))$, где A_i — это вид социоинженерного атакующего воздействия, а $S(A_i)$ — степень владения злоумышленником данным атакующим воздействием. Степень владения атакующим воздействием — это один из факторов, влияющих на оценку успешности атаки, выражающий некоторое умение злоумышленника.

Тогда, при имитации социоинженерных атакующих воздействий их успех будет определяться степенью владения им различными социоинженерными атакующими воздействиями и степенью выраженности уязвимостей атакуемого пользователя информационной системы: $p_{ij} = F\left(\left(A_i, S(A_i) \right), \left(V_j, D(V_j) \right), Q \right)$, где $S(A_i)$ — степень владения злоумышленником социоинженерным атакующим воздействием A_i, $D(V_j)$ — выраженность у пользователя уязвимости V_j, Q — матрица пороговых значений вероятностей, а p_{ij} — вероятность успеха социоинженерного атакующего воздействия злоумышленника с использованием его i-ого атакующего воздействия на j-ую уязвимость пользователя.

Описанная в статье классификация социоиженерных атак позволяет в рамках представленных моделей описать уязвимости пользователя, степени их выраженности, компетенции злоумышленника и степени их выраженности.

Заключение

В статье обозначена актуальность проблемы защиты от социоинженерных атак, представлен обзор подходов к классификации атак и рассмотрены их ограничения. Представленная классификация социоинженерных атак создает основу для построения вероятностных моделей оценки защищенности пользователей, успеха реализации атаки. В статье также представлены примеры алгебраических моделей, означивание которых может быть произведено при помощи представленной классификации. Избранный подход к классификации, ассоциированный с этапами атаки, позволяет моделировать процесс и прогнозировать его результаты. Знакомство широкого круга заинтересованных лиц с данным подходом к классификации приведет к повышению осведомленности и уровня бдительности пользователей, что, в свою очередь, уменьшит количество успешных социоинженерных атак и приведет к сбережению средств организации и граждан. Результаты данного исследования будут интересны специалистам в области управления персоналом, подготовки кадров, информационной безопасности, информационных технологий, искусственного интеллекта; руководителям, владельцам бизнеса, руководителям государственных и муниципальных органов.

Благодарности

Статья подготовлена в рамках выполнения научно-исследовательской работы государственного задания РАНХиГС и государственного задания СПБ ФИЦ РАН мол_лаба № FFZF-2024-0003.

Литература

1. Азаров А.А., Тулупьева Т.В., Суворова А.В., Тулупьев А.Л., Абрамов М.В., Юсупов Р.М. Социоинженерные атаки. Проблемы анализа. СПб.: Наука, 2016. 352 с.
2. Абрамов М.В., Тулупьева Т.В., Тулупьев А.Л. Социоинженерные атаки: социальные сети и оценки защищенности пользователей. СПб.: ГУАП, 2018. 266 с.
3. Тулупьева, Т. В. Психологические аспекты информационной безопасности организации в контексте социоинженерных атак // Управленческое консультирование. – 2022. – № 2(158). – С. 123-138.
4. Тулупьева Т.В., Абрамов М.В., Тулупьев А.Л. Модель социального влияния в анализе социоинженерных атак. Управленческое консультирование. 2021;(8), стр. 97-107.
5. Abramov M.V., Tulupyev A.L. Soft estimates of user protection from social engineering attacks: fuzzy combination of user vulnurabilities and malefactor competencies in the attacking impact success prediction // Artificial Intelligence and Natural Language. 2019. P. 47–58.
6. Albahar, M.; Almalki, J. Deepfakes: Threats and countermeasures systematic review. J. Theor. Appl. Inf. Technol. 2019, 97, 3242–3250.
7. Algarni A., Xu Y., Chan T., and Tian Y.-C., “Social engineering in social networking sites: Affect-based model,” in Internet Technology and Secured Transactions (ICITST), 2013 8th International Conference for. IEEE, 2013, pp. 508–515
8. Braun, T.; Fung, B.C.; Iqbal, F.; Shah, B. Security and privacy challenges in smart cities. Sustain. Cities Soc. 2018, 39, 499–507.
9. Chi, H.; Maduakor, U.; Alo, R.; Williams, E. Integrating deepfake detection into cybersecurity curriculum. In Proceedings of the Future Technologies Conference (FTC), Virtual Platform, San Francisco, CA, USA, 5–6 November 2020.
10. Chiew KL, Yong KSC, and Tan CL (2018b). A survey of phishing attacks: Their types, vectors and technical approaches. Expert Systems with Applications, 106: 1-20
11. Corradini, I. (2020). Redefining the Approach to Cybersecurity. In: Building a Cybersecurity Culture in Organizations. Studies in Systems, Decision and Control, vol 284. Springer, Cham. https://doi.org/10.1007/978-3-030-43999-6_3

12. De Ryck, P.; Nikiforakis, N.; Desmet, L.; Joosen, W. Tabshots: Client-side detection of tabnabbing attacks. In Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, Hangzhou, China, 8–10 May 2013.
13. Gupta, S.; Singhal, A.; Kapoor, A. A literature survey on social engineering attacks: Phishing attack. In Proceedings of the International Conference on Computing, Communication, and Automation, Noida, India, 29–30 April 2016; pp. 537–540; Yeboah-Boateng, E.O.; Amanor, P.M. Phishing, SMiShing & Vishing: An assessment of threats against mobile devices. J. Emerg. Trends Comput. Inf. Sci. 2014, 5, 297–307.
14. Ho, G.; Sharma, A.; Javed, M.; Paxson, V.; Wagner, D. Detecting credential spearphishing in enterprise settings. In Proceedings of the 26th USENIX Security Symposium, Vancouver, BC, Canada, 15–17 August 2017; pp. 469–485.
15. Hofbauer, S.; Beckers, K.; Quirchmayr, G. Defense Methods against VoIP and Video Hacking Attacks in Enterprise Networks. In Proceedings of the 10th International Conference on e-Business, Bangkok, Thailand, 23–24 November 2015; pp. 1–10.
16. Ivaturi, K.; Janczewski, L. A taxonomy for social engineering attacks. In Proceedings of the International Conference on Information Resources Management, Centre for Information Technology, Organizations, and People, Ontario, Canada, 18–20 June 2011; pp. 1–12.
17. Kalnin, s, R.; Purin, s, J.; Alksnis, G. Security evaluation of wireless network access points. Appl. Comput. Syst. 2017, 21, 38–45.;
18. Pokrovskaia, N. Social engineering and digital technologies for the security of the social capital' development. In Proceedings of the International Conference of Quality Management, Transport and Information Security, Petersburg, Russia, 24–30 September 2017; pp. 16–19.
19. Kim, H.; Yoo, D.; Kang, J.; Yeom, Y. Dynamic ransomware protection using deterministic random bit generator. In Proceedings of the IEEE Conference on Applications, Information and Network Security, Miri, Malaysia, 13–14 November 2017; pp. 1–6
20. Koyun, A.; Aljanaby, E. Social engineering attacks. J. Multidiscip. Eng. Sci. Technol. 2017, 4, 1–6.
21. Krombholz, K.; Hobel, H.; Huber, M.; Weippl, E. Advanced social engineering attacks. J. Inf. Secur. Appl. 2014, 22, 113–122.
22. Opazo, B.; Whitteker, D.; Shing, C. Email trouble: Secrets of spoofing, the dangers of social engineering, and how we can help. In Proceedings of the International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery, Guilin, China, 29–31 July 2018; pp. 2812–2817.
23. Patil, P.; Devale, P. A literature survey of phishing attack technique. Int. J. Adv. Res. Comput. Commun. Eng. 2016, 5, 198–200
24. Peotta, L.; Holtz, M.D.; David, B.M.; Deus, F.G.; De Sousa, R.T. A formal classification of internet banking attacks and vulnerabilities. Int. J. Comput. Sci. Inf. Technol. 2011, 3, 186–197
25. Pokrovskaia, N. Social engineering and digital technologies for the security of the social capital' development. In Proceedings of the International Conference of Quality Management, Transport and Information Security, Petersburg, Russia, 24–30 September 2017; pp. 16–19.
26. Salahdine, Fatima and Naima Kaabouch. "Social Engineering Attacks: A Survey." Future Internet 11 (2019): 89.
27. Suri, R.K.; Tomar, D.S.; Sahu, D.R. An approach to perceive tabnabbing attack. Int. J. Sci. Technol. Res. 2012, 1, 1–4.
28. Wang, S.; Zhu, S.; Zhang, Y. Blockchain-based mutual authentication security protocol for distributed RFID systems. In Proceedings of the 2018 IEEE Symposium on Computers and Communications, Natal, Brazil, 25–28 June 2018; pp. 74–77.
29. Wilcox, H.; Bhattacharya, M. A framework to mitigate social engineering through social media within the enterprise. In Proceedings of the IEEE International Conference on Industrial Electronics and Applications, Hefei, China, 5–7 June 2016; pp. 1039–1044
30. Xiangyu, L.; Qiuyang, L.; Chandel, S. Social engineering and Insider threats. In Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, Nanjing, China, 12–14 October 2017; pp. 25–34
31. Yeboah-Boateng, E.O.; Amanor, P.M. Phishing, SMiShing & Vishing: An assessment of threats against mobile devices. J. Emerg. Trends Comput. Inf. Sci. 2014, 5, 297–307.

APPROACHES TO CLASSIFYING SOCIAL ENGINEERING ATTACKS

Tulupyeva, Tatyana Valentinovna

Candidate of psychological sciences, associate professor
Russian Presidential Academy of National Economy and Public Administration (RANEPA), advisor to the vice-rector
Moscow, Russian Federation
St. Petersburg Federal Research Center of the Russian Academy of Sciences, Laboratory of Applied Artificial Intelligence, Senior Researcher
St. Petersburg, Russian Federation
tulupeva-tv@ranepa.ru

Abramov, Maxim Viktorovich

Candidate of technical sciences, associate professor
St. Petersburg Federal Research Center of the Russian Academy of Sciences, head of the Laboratory of applied artificial intelligence
St.Petersburg, Russian Federation
mva@dscs.pro

Azarov, Artur Alexandrovich

Candidate of technical sciences
Russian Presidential Academy of National Economy and Public Administration (RANEPA), vice-rector for science
Moscow, Russian Federation
azarov-aa@ranepa.ru

Abstract

The purpose of this article is to develop a classification of social engineering attacks that considers the specifics of the attack and its stages. The study of approaches to the classification of social engineering attacks available in the literature made it possible to cover the identified types of attacks and identify intersections and gaps in existing classifications. The developed approach to classification allows us to identify various types of attacks that consider the phasing and complexity of the impact. The introduction of pretexting at the preparation stage allows us to distinguish between targeted and non-targeted attacks, which, in combination with the selected means of contact with the victim, provide a range of different types of attacks. The presented classification of social engineering attacks creates a basis for building probabilistic models for assessing user security and the success of the attack. The chosen approach to classification, associated with the stages of the attack, allows us to model the process and predict its results. The results of this study will be of interest to specialists in the field of personnel management, training, information security, information technology, artificial intelligence; managers, business owners, heads of state and municipal departments.

Keywords:

information security, social influence, phishing, pretexting, social engineering attacks

References

1. Azarov A.A., Tulupyeva T.V., Suvorova A.V., Tulupyev A.L., Abramov M.V., Yusupov R.M. Socioinzhenernye ataki. Problemy analiza. SPb.: Nauka, 2016. 352 s
2. Abramov M.V., Tulup'yeva T.V., Tulup'yev A.L. Sotsioinzhenernyye ataki: sotsial'nyye seti i otsenki zashchishchennosti pol'zovateley. SPb.: GUAP, 2018. 266 s
3. Tulupyeva, T. V. Psikhologicheskiye aspekty informatsionnoy bezopasnosti organizatsii v kontekste sotsioinzhenernykh atak // Upravlencheskoye konsul'tirovaniye. – 2022. – № 2(158). – S. 123-138.
4. Tulupyeva T.V., Abramov M.V., Tulupyev A.L. Model' sotsial'nogo vliyaniya v analize sotsioinzhenernykh atak. Upravlencheskoye konsul'tirovaniye. 2021;(8), str. 97-107.
5. Abramov M.V., Tulupyev A.L. Soft estimates of user protection from social engineering attacks: fuzzy combination of user vulnurabilities and malefactor competencies in the attacking impact success prediction // Artificial Intelligence and Natural Language. 2019. P. 47–58.

6. Albahar, M.; Almalki, J. Deepfakes: Threats and countermeasures systematic review. J. Theor. Appl. Inf. Technol. 2019, 97, 3242–3250.
7. Algarni A., Xu Y., Chan T., and Tian Y.-C., "Social engineering in social networking sites: Affect-based model," in Internet Technology and Secured Transactions (ICITST), 2013 8th International Conference for. IEEE, 2013, pp. 508–515
8. Braun, T.; Fung, B.C.; Iqbal, F.; Shah, B. Security and privacy challenges in smart cities. Sustain. Cities Soc. 2018, 39, 499–507.
9. Chi, H.; Maduakor, U.; Alo, R.; Williams, E. Integrating deepfake detection into cybersecurity curriculum. In Proceedings of the Future Technologies Conference (FTC), Virtual Platform, San Francisco, CA, USA, 5–6 November 2020.
10. Chiew KL, Yong KSC, and Tan CL (2018b). A survey of phishing attacks: Their types, vectors and technical approaches. Expert Systems with Applications, 106: 1-20
11. Corradini, I. (2020). Redefining the Approach to Cybersecurity. In: Building a Cybersecurity Culture in Organizations. Studies in Systems, Decision and Control, vol 284. Springer, Cham. https://doi.org/10.1007/978-3-030-43999-6_3
12. De Ryck, P.; Nikiforakis, N.; Desmet, L.; Joosen, W. Tabshots: Client-side detection of tabnabbing attacks. In Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, Hangzhou, China, 8–10 May 2013.
13. Gupta, S.; Singhal, A.; Kapoor, A. A literature survey on social engineering attacks: Phishing attack. In Proceedings of the International Conference on Computing, Communication, and Automation, Noida, India, 29–30 April 2016; pp. 537–540; Yeboah-Boateng, E.O.; Amanor, P.M. Phishing, SMiShing & Vishing: An assessment of threats against mobile devices. J. Emerg. Trends Comput. Inf. Sci. 2014, 5, 297–307.
14. Ho, G.; Sharma, A.; Javed, M.; Paxson, V.; Wagner, D. Detecting credential spearphishing in enterprise settings. In Proceedings of the 26th USENIX Security Symposium, Vancouver, BC, Canada, 15–17 August 2017; pp. 469–485.
15. Hofbauer, S.; Beckers, K.; Quirchmayr, G. Defense Methods against VoIP and Video Hacking Attacks in Enterprise Networks. In Proceedings of the 10th International Conference on e-Business, Bangkok, Thailand, 23–24 November 2015; pp. 1–10.
16. Ivaturi, K.; Janczewski, L. A taxonomy for social engineering attacks. In Proceedings of the International Conference on Information Resources Management, Centre for Information Technology, Organizations, and People, Ontario, Canada, 18–20 June 2011; pp. 1–12.
17. Kalnin, s, R.; Purin, s, J.; Alksnis, G. Security evaluation of wireless network access points. Appl. Comput. Syst. 2017, 21, 38–45.;
18. Pokrovskaia, N. Social engineering and digital technologies for the security of the social capital' development. In Proceedings of the International Conference of Quality Management, Transport and Information Security, Petersburg, Russia, 24–30 September 2017; pp. 16–19.
19. Kim, H.; Yoo, D.; Kang, J.; Yeom, Y. Dynamic ransomware protection using deterministic random bit generator. In Proceedings of the IEEE Conference on Applications, Information and Network Security, Miri, Malaysia, 13–14 November 2017; pp. 1–6
20. Koyun, A.; Aljanaby, E. Social engineering attacks. J. Multidiscip. Eng. Sci. Technol. 2017, 4, 1–6.
21. Krombholz, K.; Hobel, H.; Huber, M.; Weippl, E. Advanced social engineering attacks. J. Inf. Secur. Appl. 2014, 22, 113–122.
22. Opazo, B.; Whitteker, D.; Shing, C. Email trouble: Secrets of spoofing, the dangers of social engineering, and how we can help. In Proceedings of the International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery, Guilin, China, 29–31 July 2018; pp. 2812–2817.
23. Patil, P.; Devale, P. A literature survey of phishing attack technique. Int. J. Adv. Res. Comput. Commun. Eng. 2016, 5, 198–200
24. Peotta, L.; Holtz, M.D.; David, B.M.; Deus, F.G.; De Sousa, R.T. A formal classification of internet banking attacks and vulnerabilities. Int. J. Comput. Sci. Inf. Technol. 2011, 3, 186–197
25. Pokrovskaia, N. Social engineering and digital technologies for the security of the social capital' development. In Proceedings of the International Conference of Quality Management, Transport and Information Security, Petersburg, Russia, 24–30 September 2017; pp. 16–19.

26. Salahdine, Fatima and Naima Kaabouch. “Social Engineering Attacks: A Survey.” Future Internet 11 (2019): 89.
27. Suri, R.K.; Tomar, D.S.; Sahu, D.R. An approach to perceive tabnabbing attack. Int. J. Sci. Technol. Res. 2012, 1, 1–4.
28. Wang, S.; Zhu, S.; Zhang, Y. Blockchain-based mutual authentication security protocol for distributed RFID systems. In Proceedings of the 2018 IEEE Symposium on Computers and Communications, Natal, Brazil, 25–28 June 2018; pp. 74–77.
29. Wilcox, H.; Bhattacharya, M. A framework to mitigate social engineering through social media within the enterprise. In Proceedings of the IEEE International Conference on Industrial Electronics and Applications, Hefei, China, 5–7 June 2016; pp. 1039–1044
30. Xiangyu, L.; Qiuyang, L.; Chandel, S. Social engineering and Insider threats. In Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, Nanjing, China, 12–14 October 2017; pp. 25–34
31. Yeboah-Boateng, E.O.; Amanor, P.M. Phishing, SMiShing & Vishing: An assessment of threats against mobile devices. J. Emerg. Trends Comput. Inf. Sci. 2014, 5, 297–307.