Impact Factor: 9.9 ISSN-L: 2544-980X

Направления Социальной Инженерии

МЕ Санаев [1], ША улашев [2]

Угрозы, связанные с социальной инженерией, можно классифицировать следующим образом:

Угрозы, связанные с телефоном. Телефон по-прежнему остается одним из самых популярных средств связи внутри организаций и между ними. Таким образом, он остается эффективным инструментом социальной инженерии. При разговоре по телефону нет возможности подтвердить личность собеседника. Это позволяет злоумышленникам выдавать себя за сотрудника, начальника или любого другого человека, которому можно доверить конфиденциальную или потенциально важную информацию. У жертвы насилия нет другого выбора, кроме как помочь. Особенно, если просьба об интервью кажется тривиальной.

Популярны различные методы мошенничества, направленные на кражу денег у пользователей мобильных телефонов. Это могут быть звонки или выигрыши в лотерею, СМС-сообщения, запросы на возврат денег через ошибки или сообщения о том, что у близких родственников жертвы проблемы и им необходимо немедленно перевести определенную сумму денег.

В этих случаях необходимы следующие меры безопасности:

- идентификация звонящего;
- воспользоваться услугой определения номера;
- SMS – игнорировать неизвестные ссылки в сообщении.

Угрозы по электронной почте. Многие сотрудники ежедневно получают десятки или даже сотни электронных писем через свои корпоративные и личные системы электронной почты. Конечно, при таком потоке переписки невозможно уделить достаточно внимания каждому письму. Это существенно упрощает проведение атак. Многие пользователи систем электронной почты воспринимают подобные действия как электронный аналог перемещения бумаг из одной папки в другую и спокойно относятся к получению подобных сообщений. Когда злоумышленник отправляет простой запрос по почте, его жертва часто делает то, что просят, не задумываясь о своих действиях. Электронные письма могут содержать гиперссылки, побуждающие сотрудников нарушать корпоративные правила защиты окружающей среды. Такие ссылки не всегда ведут на заявленные страницы.

Большинство мер безопасности призваны предотвратить доступ неавторизованных пользователей к корпоративным ресурсам. Если пользователь загружает вредоносную программу в корпоративную сеть, перейдя по гиперссылке, отправленной злоумышленником, он может обойти многие виды защиты. Гиперссылка также может указывать на хост со всплывающими приложениями, которым требуется информация или помощь. Как и в случае с другими видами мошенничества, наиболее эффективный способ защиты от злонамеренных атак — с подозрением относиться к нежелательной входящей электронной почте. Чтобы распространить этот подход по всей организации, политика безопасности должна включать четкие принципы использования электронной почты, включая следующие элементы:

дополнения к документам;

гиперссылки в документе;

[1] Самаркандский филиал международной школы финансовых технологий и науки
[2] Самаркандский филиал международной школы финансовых технологий и науки Студент

- запросить личную или корпоративную информацию внутри компании;
- запросы личной или корпоративной информации извне компании.

Угрозы, основанные на использовании мгновенных сообщений. Мгновенные сообщения — относительно новый метод передачи данных. Однако он уже завоевал популярность среди корпоративных пользователей. Благодаря скорости и простоте использования этот метод связи открывает широкие возможности для различных атак. Пользователи относятся к нему как к телефону и не оценивают его как потенциальную программную угрозу. Два основных типа атак, основанных на использовании службы обмена мгновенными сообщениями, — это отображение ссылки на вредоносную программу и отображение сообщения о самой программе. Конечно, обмен мгновенными сообщениями также является одним из способов запроса информации. Одной из характеристик служб обмена мгновенными сообщениями является неформальный характер общения. Наряду с возможностью сопоставления любых имен, этот фактор позволяет злоумышленнику выдать себя за кого-то другого и значительно увеличивает вероятность успешной атаки. Если компания хочет воспользоваться снижением затрат и другими преимуществами обмена мгновенными сообщениями, ей необходимо предусмотреть в корпоративной политике безопасности адекватные механизмы защиты от угроз. Чтобы иметь надежный контроль над обменом мгновенными сообщениями в корпоративной среде, необходимо соблюдение нескольких требований:

- выбрать одну платформу для обмена мгновенными сообщениями;
- определить параметры безопасности при настройке службы обмена мгновенными сообщениями;
- определить принципы установления новых отношений;
- установка стандартов выбора пароля;
- дать рекомендации по использованию мгновенных сообщений.
- Эксперты в области социальной инженерии рекомендуют организациям следующие основные методы защиты:
- разработать надежную политику классификации данных, учитывающую типы, казалось бы, безобидных данных, которые могут иметь форму конфиденциальных данных;
- обеспечить безопасность данных клиентов, используя шифрование данных или контроль доступа;
- обучение сотрудников навыкам распознавания социальных инженеров, обучение их подозрительному общению с людьми, которых они не знают лично;
- запретить сотрудникам делиться или делиться паролями;
- запретить предоставление информации, относящейся к ведомству, лицу, которое лично не известно или не проверено каким-либо образом;
- использование специальных процедур одобрения для тех, кто запрашивает доступ к конфиденциальной информации.

Используя методы социальной инженерии, крупные компании и их сотрудники часто используют сложные многоуровневые системы безопасности для защиты своих сотрудников от мошенников. Некоторые функции и обязанности таких систем перечислены ниже:

- *Физическая безопасность.* Барьеры, ограничивающие доступ к помещениям компании и корпоративным ресурсам. Не следует забывать, что ресурсы компании, например, мусорные контейнеры, расположенные за пределами территории компании, физически не защищены.
- *Информация.* Бизнес-данные: записи, почта и т. д. При анализе угроз и планировании мер защиты данных необходимо определить принципы работы с бумажными и электронными

носителями информации.

- *Приложения.* Программы, управляемые пользователем. Чтобы защитить свою среду, вам следует подумать о том, как злоумышленники могут использовать программы электронной почты, службы обмена мгновенными сообщениями и другие программы.
- *Компьютеры.* Серверы и клиентские системы, используемые в организации. Защита пользователей от прямых атак на их компьютеры путем установления строгих правил относительно того, какие программы можно использовать на корпоративных компьютерах.
- *Внутренняя сеть.* Сеть, которая взаимодействует с корпоративными системами и может быть локальной, глобальной или беспроводной. В связи с ростом популярности удаленных методов в последние годы границы внутренних сетей расширились достаточно произвольно. Сотрудники компании должны понимать, что необходимо сделать для организации безопасной работы в любой сетевой среде.
- *Периметр сети.* Граница между внутренними сетями компании и внешними, такими как Интернет или сети партнерских организаций.

Существует множество атак социальной инженерии, некоторые из которых обсуждаются ниже.

Фишинг. Фишинг – вид мошенничества в сети Интернет, целью которого является получение доступа к конфиденциальной информации пользователя, логину/паролю.

В настоящее время это одна из самых распространенных схем социальной инженерии. Широкое распространение больших объемов персональных данных, фишинг невозможен без «ветра». Самый распространенный пример фишинга — фейковое сообщение от банка или платежной системы в виде официальной информации, отправленное на электронную почту жертвы. Такие электронные письма обычно содержат ссылку на поддельную веб-страницу, которая выглядит как официальный сайт и запрашивает личную информацию (рис. 1.1). В первом случае, показанном на картинке, вместо написания имени и фамилии заказчика или пользователя пишется почтовый адрес, во втором случае, при наведении курсора мыши на указанную ссылку, это не реальный адрес(www.PayPal.com), но возможен другой адрес.

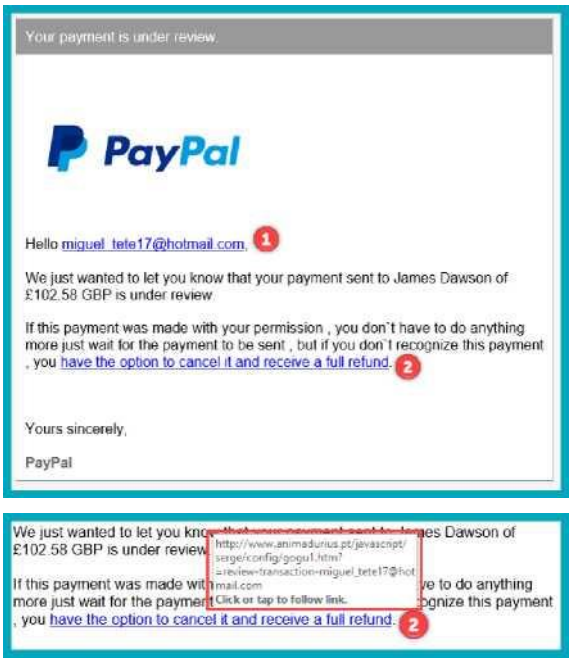

Рисунок 1.1. Пример фишинговой атаки

Ниже приведены примеры распространенных схем фишинга.

Ссылка, которой не существует. В этой форме фишинговой атаки привлекается ссылка на ссылку, содержащую сайт, похожий на ожидаемый. Например, www.PayPai.com адрес

www.PayPal.com можно отправить по адресу. При этом пользователи редко замечают наличие буквы «i» вместо буквы «l». И при переходе по ссылке www.PayPal.com Посещается сайт, похожий на веб-сайт, но являющийся подделкой, и вводятся необходимые данные платежной карты. В результате введенные данные быстро попадают в руки хакера.

Ярким примером этого является фишинговое сообщение, которое было распространено среди пользователей eBay в 2003 году. Соответственно, сообщалось, что учетные записи пользователей были заблокированы, а данные кредитных карт необходимо разблокировать. Эти электронные письма содержали ссылку на поддельную веб-страницу, похожую на официальный сайт . Ущерб от этой фишинговой атаки составил несколько сотен тысяч долларов.

Мошенничество, основанное на использовании известного корпоративного бренда. При этом виде мошенничества на электронную почту пользователя отправляются сообщения от имени известных или крупных компаний. Сообщения могут включать поздравления с победой в конкурсе, проводимом компанией. Он также попросит вас немедленно изменить данные вашей учетной записи и пароль. Подобные схемы могут быть реализованы и от имени службы технической поддержки.

Фейковые лотереи. По этой фишинговой схеме пользователь может получать сообщения о выигрыше в лотерее, проводимой какой-либо известной компанией. На первый взгляд кажется, что эти электронные письма отправлены от имени одного из старших сотрудников компании.

Поддельный антивирус и программное обеспечение безопасности. Подобное мошенническое программное обеспечение, также известное как «плавательное ПО», выглядит как антивирусное программное обеспечение, но на самом деле все наоборот. Это программное обеспечение генерирует ложные уведомления о различных угрозах и пытается вовлечь пользователя в мошеннические транзакции. Пользователь может столкнуться с ними в электронной почте, онлайн-рекламе, социальных сетях, результатах поисковых систем и даже во всплывающих окнах на рабочем столе, имитирующих системные сообщения. В приведенном ниже примере показана поддельная антивирусная программа, которая предположительно является Microsoft Security Essentials, но называет себя Security Essentials 2010.

Антивирусная программа «Security Essentials 2010».

IVR (Интерактивный голосовой ответ) или телефонный фишинг. Этот метод фишинговой схемы основан на использовании заранее записанных сообщений, которые используются для воссоздания «официальных звонков» банковских и других IVR-систем. Обычно жертва получает просьбу связаться с банком и подтвердить или обновить какую-либо информацию. Система требует аутентификации пользователя путем ввода PIN-кода или пароля. Таким образом, жертва сможет ввести всю информацию, предварительно записав ключевые фразы. Например, нажмите «1», чтобы сменить пароль, и нажмите «2», чтобы получить ответ оператора, и да.

Предлог. В этой схеме фишинга хакер выдает себя за другого человека и стремится получить конфиденциальную информацию на основе заранее подготовленного скрипта. При этой атаке проводятся соответствующие приготовления, чтобы жертва не вызвала подозрений: обнаруживается такая информация, как дата рождения, ИНН, номер паспорта или последние символы номера счета. Эта схема фишинга обычно осуществляется по телефону или электронной почте.

Quid pro quo (от лат. Quid pro quo). Эта фраза на английском языке означает *«услуга за услугу»* , и в этом типе социальной инженерии хакер связывается с компанией через корпоративную сеть или электронную почту. Часто хакер выдает себя за помощника по технической поддержке и крадет работу технического специалиста. «Помощь» в решении проблемы. Техник заставляет жертву, например, выполнять команды или устанавливать различные программы на компьютер жертвы. Исследование, проведенное в 2003 году

Программой информационной безопасности, показало, что 90% офисных работников были готовы отказаться от конфиденциальной информации, такой как пароли, ради любой услуги или платежа.

«Не увлекайся». В этом методе социальной инженерии хакер использует хранилища данных, в которых записано специальное вредоносное ПО. Для этого он оставляет контейнеры с вредоносным ПО рядом с местом работы жертвы, в общественных местах и других местах. Хранители данных формализуются в форме, приемлемой для организации. Например, этот тип атаки предполагает, что хакер оставляет компакт-диск с логотипом компании и адресом официального сайта. На поверхности этого диска может быть надпись «Заработная плата руководителей». Как только жертва заполучила эту заставку, она пытается установить ее на свой компьютер, тем самым заражая свой компьютер.

Открытый сбор данных. Методы социальной инженерии требуют не только психологических знаний, но и умения собирать необходимую информацию о человеке. Относительно новым методом получения информации является сбор ее из открытых источников, в основном из социальных сетей. Например, на таких сайтах, как «Одноклассники», «ВКонтакте», «Фейсбук», «Инстаграм» размещено много информации, которую люди не пытаются скрыть. Обычно пользователи не уделяют должного внимания вопросам безопасности и оставляют информацию и сообщения, которые могут быть использованы хакерами.

Яркий пример тому – похищение сына Евгения Касперского. То есть в ходе расследования было установлено, что график движения и маршрут следования подростка преступники узнали из публикаций на страницах социальных сетей.

Даже если вы ограничите доступ к информации на своей странице в социальной сети, нет гарантии, что пользователь никогда не станет жертвой мошенничества. Например, бразильский исследователь компьютерной безопасности показал, что он может добавить в друзья любого пользователя Facebook, используя методы социальной инженерии, в течение 24 часов. В ходе эксперимента Нельсон Новаес Нето создает фейковый аккаунт для окружающего его человека — своего начальника — для той цели, для которой он был выбран изначально. Сначала Нето отправлял запросы в друзья друзьям начальника жертвы, а затем непосредственно другу жертвы. Через 7,5 часов исследователь подружился с испытуемым. Таким образом, у исследователя появилась возможность получить личную информацию пользователя.

Атака «Посмотри через плечо» . Согласно этой атаке, злоумышленник получает информацию о жертве, заглядывая ей через плечо. Этот тип атак распространен в общественных местах, таких как кафе, автобусы, торговые центры, аэропорты и железнодорожные вокзалы.

Проведенные опросы показали, что:

- 85% участников признались, что видели конфиденциальную информацию, которую им не следовало знать;
- 82% участников признались, что информация на их экране может быть просмотрена посторонними лицами;
- 82% участников не верили, что сотрудники организации защищают свой экран от посторонних лиц.

Обратная социальная инженерия. Случай обратной социальной инженерии — когда жертва сама предоставляет свои данные злоумышленнику. Хотя это может показаться бессмысленной идеей, в большинстве случаев жертвы сами привлекают обидчика для решения своих проблем. Например, злоумышленник, работающий с жертвой, переименовывает или перемещает файл в другой каталог. И жертва, которая знает, что файл пропал, хочет побыстрее устранить эту проблему. В этой ситуации злоумышленник притворяется, что решил проблему, и вместе с решением проблемы получает логин/пароль жертвы. Кроме того, выполняя эту задачу,

злоумышленник приобретает репутацию внутри организации и увеличивает количество жертв. Определить эту ситуацию – очень непростая задача.

Известные социальные инженеры . *Кевин Митник* — один из самых известных социальных инженеров в истории. Он не только всемирно известный компьютерный хакер и эксперт по безопасности, но и автор многих книг по компьютерной безопасности, основанной на социальной инженерии. По его словам, проще получить пароль обманным путем, чем взломать систему безопасности.

Братья Бадир. Несмотря на слепоту, братья Мушид и Шади Бадир сумели реализовать в Израиле в 1990-х годах несколько крупных мошеннических схем, используя социальную инженерию и подмену голоса. В телеинтервью они заявили: «В безопасности в сети находится только тот, кто не пользуется телефонами, электричеством и ноутбуками».

Меры защиты от социальной инженерии. Злоумышленники, использующие методы социальной инженерии, часто пользуются вежливостью, ленью, вежливостью и заинтересованностью пользователей и сотрудников организаций. Предотвратить эти атаки сложно, поскольку они не знают, что их обманывают.

Атаки социальной инженерии можно определить как:

- представьтесь другом или новым сотрудником, который просит о помощи;
- представиться поставщиком, сотрудником компании-партнера или законным представителем;
- представить себя как лидер;
- выдавать себя за продавца или производителя, который устраняет уязвимость или предлагает жертве возможность что-то обновить;
- представление в качестве помощника при возникновении проблемы;
- использовать внутренний резонанс и терминологию для создания доверия ;
- добавление в «письмо» различных вредоносных программ;
- просьба повторно ввести логин/пароль в ложном всплывающем окне;
- предложить подарок за посещение сайта по логину и паролю;
- запись ключей, введенных в компьютер или программу жертвы (программы-кейлоггеры);
- размещение на рабочем столе пользователя различных регистраторов данных с помощью вредоносного ПО;
- голосовые сообщения и хак на различные голосовые вызовы.

Проблемы социальной инженерии можно увидеть во многих аспектах жизни. В частности, случаи социальной инженерии часто встречаются в массовой культуре (например, в кино). Например, в следующих фильмах есть эпизоды социальной инженерии:

Список использованных литератур

1. Eshquvvat o’g’li M.S, Zafar qizi Z.B Areas of application of artificial intelligence issn: 2181-4027 sjif: 4.995 Volume-27, Issue-2, February-2023. 61-64.
2. Eshquvvat o’g’li M.S, Naim o‘g‘li M. D, Xamrobek o’g’li N.N, Data miningda crisp-dm metodoligiyasi tasnifi Часть-11_ Том-1_ Декабрь-2023 43-46.
3. Файзиев Б.М, Бегматов Т.И, Санаев М.Э. Обратная задача по определению кинетического коэффициента в модели фильтрац ii tom tatu sf ma’ruzalar to‘plami 9 aprel 2022-yil 11-13.

4. Файзиев Б.М, Бегматов Т.И, Санаев М.Э. Идентификация коэффициента кинетики в модели фильтрации суспензии в пористой среде халқаро илмий-амалий анжуман материаллари 2022 йил, 11-12 май 360-361.
5. Eshquvvat o'g'li.M.S, Shodiyor o'g'li.Sh.J, Raxmonqul o'g'li.A.T, Ma'lumotlarni sinflashtirishda birch algoritmi ahamiyati Часть-11 Том-1 Декабрь -2023 39-42.
6. ME Sanayev, AA Quchqorov Classification of computer application software, European journal of business startups and open society Дата 2024/3/10, том 4, номер 3, страницы 62-65.
7. ME Sanayev, OF Orifov method oriented practical software classification Miasto Przyszłości 46, 210-213.
8. ME Sanayev, OF Orifov The role of text editors in editing and processing text information, European journal of innovation in nonformal education 4(3),43-47
9. SM Eshquvvat o'g'li, Kompyuter amaliy dasturiy ta'minoti tasnifi, Journal of new century innovations 48 (1), 3-8.
10. ME Санаев, КТ Бегмаматов, Топология и современные типы компьютерных сетей, Журнал, Finland" modern scientific research: topical issues, achievements and innovations" Дата 2024/5/22, Том 17, Номер 1.
11. ME Sanayev, The role, purpose and functions of information and communication technologies and systems in the economy in the process of modern education, Журнал, Finland" modern scientific research: topical issues, achievements and innovations" Дата 2024/5/22, Том 17, Номер 1.
12. ME Sanayev, Comparative analysis of the windows operating system, Журнал, Finland" modern scientific research: topical issues, achievements and innovations", Дата 2024/5/22, Том 17, Номер 1.
13. ME Sanayev, AI Ismoilov, Analysis of modern operating systems, Журнал Finland" modern scientific research: topical issues, achievements and innovations" Дата 2024/5/22, Том 17, Номер 1.
14. ME Sanayev, MB Shaymanov, Modern information technology infrastructure parts, Журнал Finland" modern scientific research: topical issues, achievements and innovations" Дата 2024/5/22, Том 17, Номер 1.
15. ME Sanayev, AI Ismoilov, The development tendencies of software products in the management of business processes in the economy, Журнал Finland" modern scientific research: topical issues, achievements and innovations", Дата 2024/5/22, Том 17, Номер 1.
16. ME Sanayev, FS Tovbayev, Familiarity with the basic concepts and features of the windows operating system, Журнал Finland" modern scientific research: topical issues, achievements and innovations", Дата 2024/5/22, Том 17 Номер 1.
17. ME Sanayev, Mobil operasion tizimlar tahlili, Журнал "germany" modern scientific research: achievements, innovations and development prospects, Дата 2024/4/20 Том 17 Номер 1.
18. ME Sanayev, AA Quchqorov, The Role of Social Networks in Human Life, Miasto Przyszłości 46, 340-341.
19. SM Eshquvvat o'g'li, Kompyuter dasturiy ta'minotiga bo'lgan talablarini tizimli tahlil qilish, Miasto Przyszłości 46, 262-265.
20. ME Sanayev, Kiber xafsizlik tushunchasi va uning vazifalari, Экономика и социум, 613-619.
21. ME Sanayev, Identifikasiya va autentifikatsiya, Экономика и социум, 620-626.