СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ КАК ИСКУССТВО ВЗЛОМА ЧЕЛОВЕКА

Шумский И. Н.

Хакасский технический институт – филиал ФГАОУ ВПО «Сибирский федеральный университет» (Республика Хакасия, г. Абакан, ул. Щетинкина, 27), e-mail: khti@khakassia.ru

Проблема обеспечения безопасности человека как носителя конфиденциальной информации возникает все более остро в связи с постоянным присутствием информационных технологий во взаимодействии человека с социумом в целом и что особенно важно с финансовыми институтами. Такое взаимодействие предполагает надежную техническую защиту персональных данных клиента от злоумышленников, но сам человек остается не защищенным от специальных техник нарушения конфиденциальности информации. Манипулятивные техники, ведущие к передаче личной конфиденциальной информации в руки злоумышленников, находят все больше носителей этой информации. В статье рассмотрен феномен социальной инженерии, его краткая история возникновения и развития, а так же популярные мошеннические техники нарушения защищенности конфиденциальной информации, среди которых фишинг, фальшивые обновления FlashPlayer, вшитые в документ Word, исполняемые файлы и другие. Поставлена проблема необходимости комплексного решения по обеспечению информационной безопасности с позиции защиты личности от социальной инженерии. Своевременное ознакомление с тенденциями в мире онлайн-угроз и социальной инженерии может помочь носителям информации избежать атак как в онлайн-коммуникации, так и угроз в реальной жизни.

Ключевые слова: социальная инженерия, безопасность, фишинг, виртуальная болезнь, конфиденциальность, манипулятивные техники, личность, киберпреступность.

SOCIAL ENGINEERING AS THE ART

Shumskiy I.N.

Khakas Technical Institute – the Branch of SFU (Abakan, Shchetinkina st., 27), e-mail: khti@khakassia.ru

The problem of providing security of a human as a holder of confidential information appears more often because of all informational technology used in bank system, in shops, government and society in general. Manipulative techniques which allows intruder to get personal confidential information are used now in more and more data carrier. Popular technologies for obtaining confidential information, such as phishing, fake updates of FlashPlayer, put in Word files, virtual disease are considered. The problem of the complex decision on maintenance of information safety is raised. Prompt acquaintance with the trends in the world of online threats and social engineering can help carriers of information to avoid attacks in both online communication and threats in real life.

The Key Words: social engineering, safety, phishing, virtual disease, confidentiality, manipulative technigues, personality, cybercrime

Социальная инженерия становится все более популярной в среде не только пользователей различных видов онлайн-коммуникации (социальные сети, электронная почта или др.), но и в повседневной жизни. Термин «социальная инженерия» используется чаще в отрицательном контексте как метод управления действиями человека без использования технических средств, основанный на использовании человеческих слабостей, как незаконный метод получения информации, однако положительный контекст термина объединяет совокупность подходов прикладных социальных наук [1].

По мнению К. Поппера, одного из теоретиков социальной инженерии, термин «социальная инженерия» был впервые введен в 1922 г. Р. Паундом в его работе «Введение в философию права». По другим сведениям термин появился в трудах С. и Б. Веббам. В отечественной литературе он появляется примерно в начале 70-х годов в работах по критике

западной социологии и социальной психологии. Для уточнения смысла данного термина обратимся к некоторым определениям, имеющимся в западной и отечественной литературе. Как пишет Ю. М. Резник в своей работе «Социальная инженерия: предметная область и границы применения» термин «социальная инженерия» употребляется главным образом для обозначения особой деятельности, ориентированной *на целенаправленное изменение и регулирование различных организационных структур* (социальных институтов, формальных организаций и др.). При этом ученый обращает внимание на то, как термин раскрывает К. Поппер, один из теоретиков социальной инженерии: «... деятельность по проектированию новых социальных институтов, а также по перестройке и управлению уже существующими социальными институтами путем частичных, постепенных реформ и изменений». Такая социальная инженерия представляется ему лишь как «частичная», «поэтапная» инженерия, имеющая ограниченную сферу применения [3,4].

В определении сущности термина "социальная инженерия" ученые (Ю. М. Резник, К. Поппер) выделяют два существенных признака:

во-первых, с данным термином связывают *организационные структуры, призванные регулировать поведение человека и контролировать его действия*;

во-вторых, *социальная инженерия реализуется при помощи специальных средств и технологий, созданных для облегчения и устранения социальных проблем, адаптации социальных групп и институтов к изменяющимся условиям, внедрения социальных новшеств*.

Веселов А.В. определяет социальную инженерию как науку междисциплинарную и в то же время как «практическую деятельность людей по регулированию общественных отношений посредством организации и развития социальных систем различного уровня сложности» [5].

Таким образом, термин "социальная инженерия" объединяет совокупность научных подходов психологии, как науки о сознании, мышлении и поведения отдельного человека и социологии, одной из задач которой является изучение подходов и методов целенаправленного изменения организационных структур.

В сфере информационной безопасности данный термин широко используется для обозначения целого ряда техник, используемых киберпреступниками. При этом их главной целью часто являются побуждение человека к раскрытию конфиденциальной информации для совершения действий направленных обход систем безопасности: «*Самая эффективная тактика сетевых атак — на нейросеть, уютно расположившуюся между монитором и спинкой офисного кресла*» [2]. На рынке программных средств доступно огромное количество продуктов для обеспечения информационной безопасности, но именно человек,

как носитель информации является самым уязвимым звеном и владеет «ключами от всех дверей»: комбинация учетных данных (логин и пароль), номер кредитной карты, данные для доступа к онлайн-банку и т.п.

Злоумышленники применяют к носителю информации манипулятивные психологические техники. Чтобы получить яркое представление о том, на что способен киберпреступник, следует посмотреть фильм «Поймай меня, если сможешь» (режиссёр Стивен Спилберг, кинокомпания DreamWorks SKG, премьера фильма 25 декабря 2002 г.). Интернет-пользователям нужно с осторожностью относиться к подозрительным действиям, даже если таковые кажутся обычными. Классическим приемом является просьба *назвать пароль, номер телефона*. Ежедневное общение, безусловно, формирует кредит доверия, позволяющий влиять на действия друг друга, при этом не замечаем происходящего. Но язык как средство общения, с точки зрения социальной инженерии, имеет несколько недостатков, так как связан с субъективным восприятием фактов, при котором можно исказить содержание информации.

Во-первых, программный подход к использованию смысловых словесных конструкций используется сегодня как инструмент манипуляции носителями информации и оказания на них влияния.

И, во-вторых, в результате данной тактики носитель информации может раскрыть персональные данные, разгласить конфиденциальную информацию, т.е. отказаться от какой-либо меры обеспечения безопасности, что, в свою очередь, устранит препятствия и откроет доступ злоумышленникам, например, к счетам банковских карт, вкладам и т.п.

Таким образом, можно применить к процессу взлома человека термин хакинг, как процесс взлома программного обеспечения, назвав его социальный хакинг. «Социальные хакеры — это люди, которые знают, как можно "взломать человека", запрограммировав его на совершение нужных действий» [6].

Связь социального фактора и хакинга кажется искусственной, но онлайн-атаки основаны на таких же принципах, что и офлайновое мошенничество, это:

−*принцип возвратности* (если я окажу тебе услугу, ты окажешь услугу мне),

−*принцип социальной проверки* (вы оцениваете свое поведение как правильное, если наблюдаете такое же поведение у большинства),

−*принцип преклонения перед авторитетами* (проявление большей степени доверия к сотруднику полиции, врачу, сотруднику технической поддержки).

Социнженер, как специалист управления действиями человека, владеет *манипулятивными техниками управления для* получения желаемого ответа, создавая контекст ("канву") для формирования правдоподобной легенды, которая смогла бы создать

ощущение срочности. Для опытных специалистов в сфере социальной инженерии не составит труда обойти рациональное мышление человека, им понадобится немного времени, чтобы добиться преимущества и получить от носителя информации необходимые данные.

В современном мире виртуальной коммуникации онлайн-мошенники используют различные техники для незаконного получения информации и прибыли. Как уже упомянуто выше, для подобного рода схем используются принципы, похожие на те, что используются в реальной жизни и использование Интернета данный тип атак превращает в беспроигрышную лотерею: даже если небольшая часть от общего большого числа потенциальных жертв "*попадется на удочку"*, это все равно означает огромную прибыль для организации или человека, стоящего за атакой.

Сегодня одним из самых распространенных методов получения конфиденциальной информации является фишинг (термин образован от игры слов password harvestingfishing – *ловля паролей*). Фишинг можно охарактеризовать как тип компьютерного мошенничества, который использует принципы социальной инженерии с целью получения от жертвы конфиденциальной информации. Киберпреступники, как правило, осуществляют свои действия при помощи электронной почты, сервисов мгновенных сообщений или SMS. Они посылают фишинговое сообщение, в котором напрямую просят пользователя предоставить информацию (путем ввода учетных данных в поля сайта-подделки, скачивания вредоносных программ при нажатии на ссылку и т.д.). В итоге, злоумышленники получают желаемое при полном неведении со стороны носителя информации. Ещё некоторое время назад факт заражения компьютера вирусом был весьма очевиден: пользователь видел странные сообщения, иконки, картинки. Однако современные вредоносные программы для доступа к системам носителей информации остаются невидимыми до момента выполнения поставленной задачи. Кроме фишинга, наиболее популярны фальшивые обновления FlashPlayer и других популярных программ, «вшитые» в документ Word, исполняемые файлы.

Распространены так же и атаки, которые не всегда попадают в категорию компьютерного мошенничества, например, схема *виртуальное похищение*, в которой в качестве средства связи используется телефон: злоумышленники звонят жертве и говорят, что член семьи был похищен и для его освобождения требуется незамедлительно заплатить выкуп. Преступник создает ощущение срочности и страха, абонент выполняет требования мошенника, даже не убедившись, действительно ли похищен кто-то из родственников. Похожая схема (*виртуальная болезнь)* популярна при атаках на пожилых людей: абоненту звонят, якобы из поликлиники, говорят, что в недавних анализах есть признаки опасного заболевания и нужно незамедлительно лечение для спасения жизни, разумеется, платное.

После оплаты, конечно же, никто никого не оперируют, потому что никакой болезни и не было.

Таким образом, многовариативность видов мошенничества, направленных на кражу конфиденциальной информации у человека для обхода систем информационной безопасности компьютера подтверждает, что своевременное информирование – это ключевой защитный механизм, необходимый для пользователей средств современной коммуникации, которые должны следить за новинками в мире информационной безопасности, а также знать о распространенных тактиках интернет-мошенников. Важно помнить, что любая публично доступная информация в соцсетях (ВКонтакте, Instagram, Facebook, Twitter, Foursquare и др.) может указать на местонахождение, предоставить персональные данные, сведения из личной жизни и др.

Потенциальными возможностями по частичному решению проблемы обеспечения информационной безопасности обладает система образования, в силу того что ее кадровый потенциал «отличается от многих других особыми личностными качествами – качествами педагогов, среди которых субъектность, способность к саморазвитию, самоактуализации, самообразованию и неравнодушие к судьбе подрастающего поколения», включением специальных дисциплин [7]. Содержание таких дисциплин должно носить междисциплинарных характер интегрируя содержание психологи, педагогики, социологии, философии и информатики в единый комплекс, посвященный проблемам обеспечения безопасности человека, как на уровне личности, так и на уровне использования им компьютера при различных социальных и профессиональных взаимодействиях.

Комплексное решение по обеспечению информационной безопасности должно начинаться на уровне получения еще дошкольного образования и становиться насущной необходимостью. Ознакомление с тенденциями в мире онлайн-угроз и методами социальной инженерии может помочь носителям информации избежать атак и их последствий как при онлайн-коммуникации, так и в реальной жизни.

Литература

1. Информационный ресурс, свободная энциклопедия. [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Социальная_инженерия

2. Хакер. Безопасность, разработка, DevOps. [Электронный ресурс]. – Режим доступа: https://xakep.ru/2015/06/23/pentesting-197/.

3. Резник Ю.М. Социологические исследования [Электронный ресурс]. – Режим доступа: http://ecsocman.hse.ru/data/888/223/1217/011_Reznik.pdf – Заглавие с экрана.– (Дата обращения: 15.01.2018).

4. Резник Ю.М. Социальная инженерия в системе социологического образования [Электронный ресурс]. – Режим доступа: http://ecsocman.hse.ru/data/134/199/1217/003_reznik.pdf. – Заглавие с экрана.– (Дата обращения: 15.01.2018).

5. Веселов А.В. Социальная инженерия: сущность и парадигмальная методология : : автореферат дис. ... кандидата философских наук : 09.00.01 / Веселов Александр Васильевич. – Москва, 2012. – 32 с.

6. Кузнецов М.В. Социальная инженерия и социальные хакеры / М. В. Кузнецов, И. В. Симдянов. — СПб.: БХВ-Петербург, 2007. — 368 с.

7. Янченко И.В. Информационный и технологический вызовы образованию как точки роста // Актуальные проблемы гуманитарных и естественных наук. 2016. № 2-5. С. 8-10.