УДК 004 **Информационные технологии**

Майданский Александр Дмитриевич, *студент*
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
E-mail hanako@internet.ru

ОСНОВНЫЕ МЕХАНИЗМЫ ПОЛУЧЕНИЯ ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Аннотация: В наше время информационная безопасность является одной из наиболее важных тем, и защита данных - задачей первостепенной важности. Однако, кроме технических средств защиты, существует еще один способ получения доступа к информации - социальная инженерия. Этот метод получения информации через манипуляцию людьми используется всё чаще и становится наиболее эффективным способом атак на данные и информацию. В данной статье мы рассмотрим основные механизмы, которые социальные инженеры используют для получения доступа к информации, такие как фишинг, социальная инженерия через телефонные звонки, взлом паролей, физический доступ, взлом почты и почтовых ящиков, а также использование вредоносного ПО. Разберем каждый механизм подробно, приведем примеры атак и рассмотрим методы защиты от них. Знание этих механизмов поможет читателям защитить свою информацию и данные от потенциальных угроз со стороны социальных инженеров.

Ключевые слова: социальная инженерия, фишинг, социальная инженерия через телефонные звонки, взлом паролей, физический доступ, взлом почты, вредоносное ПО, защита данных, информационная безопасность.

Annotation: Nowadays, information security is one of the most important topics, and data protection is a task of paramount importance. However, in addition to

technical means of protection, there is another way to gain access to information - social engineering. This method of obtaining information through the manipulation of people is being used more and more often and is becoming the most effective way to attack data and information. In this article, we will look at the main mechanisms that social engineers use to gain access to information, such as phishing, social engineering through phone calls, cracking passwords, physical access, hacking mail and mailboxes, and using malware. We will analyze each mechanism in detail, give examples of attacks and consider methods of protection against them. Knowing these mechanisms will help readers protect their information and data from potential threats from social engineers.

Key words: social engineering, phishing, social engineering through phone calls, password cracking, physical access, email hacking, malware, data protection, information security.

Социальная инженерия - это процесс влияния на людей с целью получения доступа к конфиденциальной информации или выполнения действий в интересах злоумышленника. Социальная инженерия может включать в себя использование различных методов и техник, таких как манипуляция, обман, внушение доверия и убеждение. Целью социальной инженерии является не взлом технических средств защиты, а получение доступа к информации путем воздействия на человеческий фактор [1].

Механизмы социальной инженерии

Использование социальной инженерии - это один из наиболее эффективных способов получения доступа к информации, так как часто люди являются слабым звеном в системе безопасности. Рассмотрим подробнее основные механизмы, которые социальные инженеры используют для достижения своих целей:

1. Фишинг,
2. Социальная инженерия через телефонные звонки,
3. Взлом паролей,

4. Физический доступ,
5. Взлом почты и почтовых ящиков,
6. Использование вредоносного ПО.

В целом, социальная инженерия - это опасный инструмент для получения доступа к конфиденциальной информации. Важно понимать, какие методы используют злоумышленники, чтобы защитить себя и свои данные.

1. Фишинг

Фишинг - это метод атаки, который зависит от манипуляции жертвой с помощью социальных инженерных методов. Фишинг-атаки могут быть очень хитрыми и обманчивыми, так как злоумышленники могут использовать копии настоящих веб-сайтов, электронных писем и даже телефонных номеров, чтобы создать иллюзию подлинности.

Самые распространенные формы фишинга - это атаки на электронную почту и атаки на социальные сети. В первом случае злоумышленник может отправить электронное письмо, которое кажется официальным сообщением от банка, сервиса электронной почты, интернет-магазина или другого веб-сайта, который вы доверяете. Электронное письмо может содержать ссылку на сайт, который выглядит как оригинальный сайт компании, но на самом деле создан злоумышленником. При переходе на этот сайт жертва будет вынуждена ввести свои логин и пароль или другие конфиденциальные данные.

В атаках на социальные сети злоумышленники могут создавать фальшивые аккаунты или использовать скомпрометированные аккаунты, чтобы обмануть пользователей и получить доступ к их личной информации. Например, злоумышленник может создать фейковый профиль на Facebook, притворяться вашим другом или родственником и попросить вас предоставить личную информацию или даже отправить деньги.

Одним из способов защиты от фишинг-атак является использование антивирусного программного обеспечения и антиспам фильтров, которые могут блокировать вредоносные ссылки и электронные письма. Также рекомендуется внимательно проверять электронные сообщения на наличие грамматических и

орфографических ошибок, а также на предмет подозрительных деталей, таких как неправильный адрес отправителя или неожиданные запросы на обновление личной информации.

2. Социальная инженерия через телефонные звонки

Социальная инженерия через телефонные звонки - это метод манипулирования людьми, когда злоумышленник звонит на телефон и выдает себя за представителя компании, банка или правительства с целью получить конфиденциальную информацию, такую как пароли, пин-коды и другие личные данные. Злоумышленники могут использовать различные методы, такие как угрозы или обман, чтобы убедить жертву раскрыть информацию.

Примеры атак социальной инженерии через телефонные звонки могут включать в себя звонки от злоумышленников, которые выдают себя за работников банка или представителей технической поддержки компьютера. Они могут просить жертву подтвердить свои личные данные или попросить установить вредоносное ПО на компьютере, которое может использоваться для кражи информации.

Для защиты от социальной инженерии через телефонные звонки следует быть осторожными при предоставлении личной информации. Если вы получаете подозрительный звонок, не следует раскрывать никакую информацию, а лучше перезвонить на известный вам номер, чтобы убедиться в том, что звонок действительно был инициирован представителем компании или организации.

3. Взлом паролей

Взлом паролей – это процесс получения несанкционированного доступа к системе или учетной записи, используя украденные или подобранные пароли. Злоумышленники могут использовать различные методы для взлома паролей, включая перебор паролей, использование словарных атак, фишинг, сетевой перехват и другие техники.

Для взлома паролей могут использоваться специальные программы, называемые "взломщиками паролей". Они могут использоваться для автоматизации перебора паролей и словарных атак. Кроме того,

злоумышленники могут использовать уязвимости в программном обеспечении, чтобы получить доступ к базам данных паролей или к файлам, содержащим хеши паролей.

Для защиты своих паролей следует использовать сильные пароли, состоящие из букв, цифр и символов, а также менять их регулярно. Не следует использовать одинаковые пароли для различных сервисов или учетных записей. Дополнительным уровнем защиты может быть использование двухфакторной аутентификации, которая требует ввода кода, полученного на телефон или другое устройство, помимо ввода пароля.

4. Физический доступ

Физический доступ - это процесс получения несанкционированного доступа к объекту, зданию или помещению с целью получения информации или совершения кражи, или других преступлений. Злоумышленники могут использовать различные методы, чтобы получить физический доступ, например, использование поддельных удостоверений личности, взлом замков, использование багажа и другие техники.

Примеры атак с использованием физического доступа включают в себя взлом замков, взлом дверей и окон, использование социальной инженерии для получения доступа к помещению, кражу компьютеров и другое.

Для защиты своего физического доступа следует использовать безопасные замки, ключи и другие средства физической защиты, такие как системы видеонаблюдения, охранная сигнализация и прочие. Следует также обучать сотрудников правилам безопасности и проверять удостоверения личности посетителей перед предоставлением им доступа к помещению [2].

5. Взлом почты и почтовых ящиков

Взлом почты и почтовых ящиков является еще одним распространенным видом атак социальной инженерии. Как правило, злоумышленник получает доступ к электронной почте жертвы с помощью украденных учетных данных, которые были получены через фишинг или взлом компьютера жертвы.

Для взлома почты могут использоваться различные инструменты,

например, брутфорс (перебор паролей), скиммеры (программы, которые перехватывают вводимые данные), шпионские программы и т.д.

Чтобы защитить свою почту и почтовый ящик от взлома, необходимо соблюдать ряд мер предосторожности. Важно использовать надежные пароли, которые содержат буквы разного регистра, цифры и символы. Кроме того, необходимо использовать двухфакторную аутентификацию, которая предоставляет дополнительный уровень защиты.

Также важно не отвечать на подозрительные письма, не открывать вложения от незнакомых отправителей и не переходить по ссылкам, которые приходят в электронной почте. Если вы получаете письма с подозрительным содержанием, лучше всего удалить их немедленно, не открывая их.

Наконец, необходимо регулярно проверять активность своего почтового ящика, чтобы быстро выявлять любые подозрительные действия. Если вы замечаете какие-либо необычные активности в своей почте, необходимо сразу же обратиться к провайдеру электронной почты или специалистам по компьютерной безопасности.

6. Вредоносное ПО

Вредоносное ПО (программное обеспечение) – это программы, которые были созданы для нанесения вреда компьютеру или сети, в которой он находится. Они могут причинить много различных видов вреда, от украденной конфиденциальной информации до повреждения системных файлов и приведения к сбою всей системы [5].

Основные виды вредоносного ПО включают в себя вирусы, троянские программы, черви, руткиты и шпионское ПО. Каждый из них имеет свои уникальные характеристики и способы работы.

1. Вирусы - это программы, которые прикрепляются к другим файлам и заражают их. Когда зараженный файл запускается, вирус начинает выполнять свои вредоносные действия, например, копировать себя на другие файлы и отправлять личные данные злоумышленникам [4].

2. Троянские программы - это программы, которые скрывают свое

настоящее назначение и представляются как полезные или необходимые приложения. Когда пользователь устанавливает их на свой компьютер, они могут начать выполнять различные действия без ведома пользователя, например, отправлять конфиденциальную информацию злоумышленникам.

3. Черви - это программы, которые распространяются по сети без необходимости присоединения к другим файлам. Они могут проникать в систему и запускаться автоматически, когда пользователь открывает инфицированный файл. Они могут также использовать сетевые ресурсы для распространения себя на другие компьютеры [6].

4. Руткиты - это программы, которые скрывают свое наличие на компьютере и могут контролировать его действия. Они могут проникать в компьютеры через уязвимости в системе безопасности и обходить антивирусные программы, а также получать удаленный доступ к компьютеру [3].

5. Шпионское ПО - это программы, которые устанавливаются на компьютер без согласия пользователя и собирают личную информацию о его действиях, например, пароли, данные банковских карт, историю посещения веб-сайтов и т.д.

Чтобы защитить свой компьютер от вредоносного ПО, рекомендуется использовать антивирусные программы и обновлять их регулярно, а также не открывать подозрительные вложения в электронных письмах и не устанавливать программы из ненадежных источников.

Один из самых распространенных способов заражения компьютера вредоносным ПО является открытие вредоносного вложения в электронном письме. Поэтому важно быть осторожным при открытии писем от неизвестных отправителей и никогда не открывать вложения, которые могут выглядеть подозрительно.

Для защиты своего компьютера от вредоносного ПО, рекомендуется установить антивирусное ПО и обновлять его регулярно. Также важно обновлять операционную систему и другие программы на компьютере, так как обновления могут содержать исправления уязвимостей, которые могут быть использованы

злоумышленниками. Кроме того, следует быть осторожным при посещении незнакомых сайтов и не устанавливать программы из ненадежных источников.

В данной статье были рассмотрены основные механизмы получения информации при использовании социальной инженерии. Мы описали, что такое фишинг и как он работает, как происходит социальная инженерия через телефонные звонки, как взламываются пароли, как осуществляется физический доступ, как взламывается почта и почтовые ящики, а также как работает вредоносное ПО.

Все эти механизмы социальной инженерии могут привести к получению злоумышленником доступа к нашей личной информации, что может привести к различным негативным последствиям, включая утечку личных данных, финансовые потери и т.д.

Поэтому, важно знать о таких механизмах и принимать меры для защиты своей информации. Мы описали некоторые из таких мер, включая использование надежных паролей, не раскрытие личной информации по телефону или по почте, использование антивирусных программ и т.д.

Наконец, следует отметить, что защита своей информации является важной задачей в нашем цифровом мире. Знание механизмов социальной инженерии и принятие соответствующих мер защиты помогут нам сделать нашу информацию более безопасной и защищенной.

Библиографический список:

1. Андреев А.А. Социальная инженерия: подходы к определению и классификации // Наука и технологии. - 2018. - Т. 1. - № 1. - С. 17-22.

2. ГОСТ Р ИСО/МЭК 27001-2013 (ISO/IEC 27001:2013) Информационная технология. Технологии обеспечения безопасности. Системы управления информационной безопасностью. Требования.

3. Гельфанд А. М. и др. Разработка модели распространения самомодифицирующегося кода в защищаемой информационной системе //Современная наука: актуальные проблемы теории и практики. Серия:

Естественные и технические науки. – 2018. – №. 8. – С. 91-97.

4. Гельфанд А. М. СПОСОБЫ ВЫБОРА СТЕГОКОНТЕЙНЕРОВ ДЛЯ ПЕРЕДАЧИ ДАННЫХ //Региональная информатика и информационная безопасность. – 2020. – С. 260-262.

5. Штеренберг С. И., Красов А. В. Варианты применения языка ассемблера для заражения вирусом исполнимого файла формата ELF //Информационные технологии и телекоммуникации. – 2013.

6. Штеренберг С. И., Красов А. В., Цветков А. Ю. Компьютерные вирусы. – 2015.