С.В. Петерс, Д.А. Фролов, В.И. Громов

ИССЛЕДОВАНИЕ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ, КАК ОДНОЙ ИЗ САМЫХ СЕРЬЁЗНЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ И ЛИЧНЫХ ДАННЫХ СОВРЕМЕННОГО ЧЕЛОВЕКА, И СПОСОБОВ БОРЬБЫ С НЕЙ.

Россия, г. Пенза, Пензенский государственный технологический университет

The article discusses social engineering and ways to combat it. The author describes in detail the methods of work of social engineers and talks about the latest developments in this field. In the end, the author suggests ways to protect personal data from intruders.

В современном мире с каждым годом всё больше и больше персональных данных хранится в сети Интернет. Большинство людей не отдают себе отчёт в том, каким количеством информации о них владеют разные компании: логины, пароли, дебетовые карты, паспортные данные и т.д. Причём многие организации собирают информацию даже о предпочтениях своих клиентов, путём сохранения поисковых запросов и использования их в целях улучшения качества обслуживания.

В 2021 году крупным компаниям приходится использовать технологию *BIG DATA*, чтобы справляться с таким потоком данных. Всё это приводит к тому, что в двадцать первом веке информация – это самый продаваемый продукт. Опустим факторы моральности и законности таких действий, просто вспомним, что всё чаще происходят “взломы” облачных хранилищ и публичных страниц известных личностей с целью обогащения путём шантажа этих людей или мошенничества от их лица. Учитывая, что такое происходит довольно часто, каждому человеку стоит задуматься об обеспечении безопасности своих данных.

Информационная безопасность — практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. [4]

BIG DATA - обозначение структурированных и неструктурированных данных огромных объёмов и значительного многообразия, эффективно обрабатываемых различными программными средствами, предназначенными для их анализа и систематизации. [2]

Среди людей, работающих в сфере информационной безопасности (далее ИБ), бытует мнение, что самой уязвимой точкой современных систем является человек. Чтобы понять так ли это, обратимся к цифрам. Согласно заявлению управляющего директора международной школы ИБ “*HackerU*”, 76% работающих россиян – это люди старше 30 лет, которые получили образование до активного развития цифровых технологий, т.е. гораздо хуже адаптированы к процессу защиты собственных данных. Такие люди становятся лёгкой добычей специалистов социальной инженерии.

Социальная инженерия – это совокупность психологических и социологических приемов, методов и технологий, которые позволяют получить конфиденциальную информацию, используя в качестве уязвимости систем человеческий фактор. [1]

По данным ФинЦЕРТа (подразделение центрального банка РФ по борьбе с кибератаками) на конец 2020 года, общее количество инцидентов, связанных с социальной инженерией, выросло на 88% по сравнению с предыдущим годом. При этом следует учитывать, что только на конец 2019 года ущерб российских компаний составил 1,26 млрд руб.

Исходя из этого, можно сделать вывод, что социальная инженерия одна из самых серьёзных угроз безопасности информационных систем и личных данных

современного человека.

Как гласит русская народная пословица: ”Врага лучше знать в лицо”, поэтому рассмотрим основные виды и методики социальной инженерии. Среди главных методов социальной инженерии выделяются: «троянский конь», претекстинг, «дорожное яблоко», фишинг, кви про кво. Расскажем о них подробнее.

«Троянский конь» - используется любопытство человека и его желание получить выгоду. На *E-Mail* жертвам отправляются письма, в которых содержится интересное вложение. [1] Метод используется, чтобы вынудить человека кликнуть по баннеру во вложении, скачать заражённый файл и т.д. Итог всегда один: компьютер пользователя заражается вредоносной программой, которую злоумышленник использует в своих интересах.

Самым ярким примером является “угон” *YouTube* канала “*IKOTIKA*” и дальнейшая его перепродажа. Вот как эту ситуацию прокомментировал владелец канала: «Мне пришло сообщение ВКонтакте с предложением якобы от рекламодателя. К письму был приложен *word* документ с техническим заданием. Как только я скачал и открыл этот документ, мой ноутбук просто выключился. Доступ к каналу после этого я потерял. Как мне потом объяснили, в этом документе был вирус, который полностью просканировал мою систему, отправив все логины и пароли злоумышленникам». Позже канал вернули законному владельцу, но это скорее исключение из правил, поэтому каждому человеку нужно более внимательно и осознанно подходить к защите своих личных данных!

«Претекстинг» - действие, которое совершается по предварительно подготовленному сценарию. [1] Цель состоит в том, чтобы человек выдал важные сведения или совершил конкретные действия. В основном такой вид мошенничества применяется при помощи телефонных обзвонов большого количества пользователей.

Авторы предполагают, что хотя бы раз в жизни каждому читателю звонили с неизвестного номера, представлялись сотрудниками службы безопасности банков и задавали какие-то странные вопросы. Это стандартная схема претекстинга, по итогам которой вы сообщите код от своей банковской карты злоумышленникам!

Так же стоит отметить, что с тех пор, как в банках появилась функция подтверждения финансовых операций с помощью биометрии, стало очень опасно говорить слово “ДА” при разговоре с неизвестными абонентами. Обычно в начале такого звонка, говорят что-то вроде: “Здравствуйте, я представитель компании Сбербанк, Василий Пупкин. Иван Иванов, это вы?” или же “… вы подтверждаете, что это вы?”. В таких ситуациях ни в коем случае нельзя отвечать “ДА” или “ПОДТВЕРЖДАЮ”. Ваш ответ будет записан и использован, чтобы вывести деньги с вашего счёта! Если вы не уверены, что это мошенник, то отвечайте зеркально: “Это вы? Это я” или же “Иван Иванов? Иван Иванов!”. Если вы возьмёте это себе за правило, то сильно обезопасите себя и свои данные.

«Дорожное яблоко» - адаптация «троянского коня», для которой требуется физический носитель информации, например *USB* накопитель. [1] Метод основан на жадности и любопытстве человека. Заражённую флэшку достаточно подкинуть человеку в автомобиль или на рабочее место. Как только жертва вставит накопитель к себе в ПК, вредоносная программа передаст все ваши данные социальному инженеру. Стоит отметить, что данный метод в основном является направленной атакой на заранее выбранную цель.

Фишинг – это метод рассылки якобы официальных писем от крупных компаний со ссылкой на поддельный сайт, являющийся точной копией официального (далее зеркало). [1] Обычно отправители таких писем преследуют две цели: добиться того чтобы пользователь ввёл данные своей карты при “покупке”, или чтобы человек авторизовался на сайте. В итоге у жертвы либо уводят аккаунт, либо деньги с карты.

Начиная с апреля 2021 года, в мире значительно повысилась опасность фишинга. Дело в том, что 3 апреля 2021 года в *DarkNet* были выложены данные более полумиллиарда аккаунтов пользователей Facebook. Поэтому, если у вас имеется страница в этой социальной сети, авторы рекомендуют проверить доступ к ней, а так же ожидать наплыва фишинговых писем на электронные почты. Будьте внимательны и осторожны!

DarkNet - это скрытая сеть, соединения которой устанавливаются при помощи нестандартных протоколов и портов. На сайты такой сети невозможно попасть из обычного браузера, а используется *DarkNet* зачастую для разного рода незаконных сделок и операций. [3]

«Кви про кво» - это метод, используемый для атак на компании. [1] Злоумышленники представляются сотрудниками техподдержки и расспрашивают сотрудников на тему неисправностей. Если таковые имеются, то они предлагают помочь их устранить. После того как работник выполняет рекомендации “техподдержки”, появляются уязвимости, через которые профессиональные хакеры могут воздействовать на корпоративную сеть компании.

Чтобы выяснить, какие целевые группы наиболее подвержены атакам социальных инженеров, мы провели опрос, в процессе которого людям было задано 2 вопроса: “Как часто вам звонят мошенники?” и “Попадались ли вы хоть раз на их уловки?”. В опросе приняли участие 5000 человек города Пензы разных возрастных групп. Проанализировав ответы и сгруппировав их по возрасту, мы выяснили, что в первую группу риска входят люди старше 55 лет (86,8% из них звонят не менее двух раз в неделю, 57,9% хоть раз выдавали мошенникам свои данные), на втором месте дети от 14 до 17 лет (54,6% и 39,8% соответственно), на третьем месте идут люди от 35 до 54 лет (74,9% и 32,4% соответственно), ну и наиболее адоптированы к нападкам мошенников люди от 18 до 34 лет (76,4% и 18,6% соответственно).

Исходя из выше перечисленных данных, мы собрали список рекомендаций по обеспечению безопасности личных:

1) Объяснять

Начните с себя: расскажите своим бабушкам и дедушкам, а возможно и родителям, что им могут звонить мошенники, а так же чего они добиваются и какими способами.

2) Просвещать

Если вы учитель, а ещё лучше директор школы, организуйте лекции для детей, на которых им расскажут всё о мошенниках (см. п.1). Аналогичные действия стоит проводить крупным компаниям, сотрудники которых всегда в группе риска.

3) Двухфакторная аутентификация

Чтобы обезопасить свои личные данные, стоит настроить двухэтапный вход в соцсети. Тогда кроме логина и пароля от вас потребуется защитный код, который будет приходить на ваш номер телефона. Даже если злоумышленники узнают ваши логин и пароль, кода они знать не будут.

4) Спам

По возможности, настройте функцию фильтрации спам писем на электронной почте, а также спам звонков у оператора сотовой связи.

5) Виртуальная карта

Закажите себе в банке виртуальную карту, и используйте её только в случае оплаты товаров или услуг через интернет. Даже если данные вашей карты попадут к социальным инженерам, то денег на ней всё равно не будет.

Таким образом, необходимо не только бережно относится к конфиденциальности своих личных данных, но просвещать других людей по этому поводу. Ведь если

каждый сделает хотя бы маленький вклад в такое большое дело, цифровая эпоха может стать гораздо безопаснее!

1. Кузнецов М.А., Симдянов И.В., Социальная инженерия и социальные хакеры – Москва, «ЭКСМО», 2019 – С. 17-76.
2. Фаулер М.Н., Садаладж П.Д., NoSQL: новая методология разработки нереляционных баз данных – М.: «Вильямс», 2018 – С. 213.
3. Фролов А.А., Сильнов Д.С., Исследование механизмов распространения запрещенного содержимого в Darknet – Современные информационные технологии и IT образование/Электронный сборник, 2017 – С. 3-4.
4. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. — Рн/Д: Феникс, 2017. — С 3-7.