Файзуллин Рамазан Рустамович
студент 3 курс, Институт истории и государственного управления
Башкирский государственный университет
Россия, г.Уфа
Байрушин Федор Тимофеевич
доцент кафедры «Управления информационной безопасностью»
Институт истории и государственного управления
Башкирский государственный университет
Россия, г.Уфа

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ - ВЗЛОМ ЧЕЛОВЕКА

Аннотация: *Социальная инженерия является наукой и искусством взлома человеческого сознания и становится все более популярной в связи с повышением роли социальных сетей, электронной почты или других видов онлайн-коммуникации в нашей жизни. В сфере информационной безопасности данный термин широко используется для обозначения ряда техник, используемых киберпреступниками.*

Ключевые слова: *социальная инженерия, фишинг, киберпреступник, безопасность.*

Annotation*: Social engineering is the science and art of hacking the human mind and is becoming more popular in view of the increasing role of social networks, e-mail or other types of online communication in our lives. In the field of information security, the term commonly used to describe several techniques used by cybercriminals.*

Keywords: *social engineering, fishing, cyber criminals, security.*

Социальная инженерия — это метод управления действиями человека без использования технических средств. Метод основан на использовании слабостей (человеческого фактора) и считается очень эффективным методом. Зачастую социальную инженерию рассматривают как незаконный метод получения информации, но социальную инженерию

можно также использовать и в законных целях — не только для получения информации, но и для совершения действий конкретным человеком. Сегодня социальную инженерию зачастую используют в интернете для получения закрытой информации, или информации, которая представляет большую ценность.

Большинство киберпреступников не станут тратить время на осуществление технологически сложных приемов взлома, если необходимые сведения можно получить, используя навыки в области социнженерии. Более того, существует множество сайтов, где описаны принципы работы подобных техник и причины их успеха. Используем речь каждый день, мы влияем на действия друг друга, хотя часто не замечаем этого. Но язык с точки зрения социальной инженерии имеет несколько недостатков, так как он связан с нашим субъективным восприятием фактов, при котором мы можем опустить некоторые части истории, исказить смысл или сделать некоторые обобщения. Нейролингвистическое программирование, которое изначально было создано для лечебных целей, сегодня используется как инструмент манипуляции жертвами и оказания на них влияния с целью побудить их выполнить действия, ведущие к успеху атаки. В результате данного метода жертва может сообщить свой пароль, разгласить конфиденциальную информацию, отказаться от какой-либо меры обеспечения безопасности, то есть, может сделать все что угодно, чтобы убрать препятствия на пути злоумышленников.

Сегодня одним из самых распространенных методов получения конфиденциальной информации является фишинг (термин образован от игры слов password harvesting fishing — «ловля паролей»). Фишинг можно охарактеризовать как тип компьютерного мошенничества, который использует принципы социальной инженерии с целью получения от жертвы конфиденциальной информации. Киберпреступники обычно осуществляют свои действия при помощи электронной почты, сервисов мгновенных

сообщений или SMS, посылая фишинговое сообщение, в котором напрямую просят пользователя предоставить информацию (путем ввода учетных данных в поля сайта-подделки, скачивания вредоносного ПО при нажатии ссылки и т.д.), благодаря чему злоумышленники получают всю нужную для них информацию.

Практически каждый день появляются новые схемы мошенничества. Большинство людей может самостоятельно научиться распознавать мошеннические сообщения, познакомившись с их некоторыми отличительными признаками. Чаще всего фишинговые сообщения содержат:

- сведения, вызывающие беспокойство, или угрозы;

- обещания огромного денежного приза с минимальными усилиями или вовсе без них;

- запросы о добровольных пожертвованиях от лица благотворительных организаций;

- имитацию повреждённого или неправильно перекодированного текста;

- адрес несуществующего почтового ящика, указанного в качестве адреса отправителя.

Популярные фишинговые схемы:

- несуществующие ссылки;

- мошенничество с использованием брендов известных корпораций;

- ложные антивирусы и программы для обеспечения безопасности

- телефонный фрикинг (фрикинг (англ. phreaking) — термин, описывающий эксперименты и взлом телефонных систем с помощью звуковых манипуляций с тоновым набором. Эта техника появилась в конце 50-х в Америке).

- плечевой серфинг (англ. *shoulder surfing*) включает в себя наблюдение личной информации жертвы . Этот тип атаки распространён в общественных

местах, таких как кафе, торговые центры, аэропорты, вокзалы, а также в общественном транспорте.

Опрос ИТ-специалистов в белой книге о безопасности показал, что:

- 85 % опрошенных признались, что видели конфиденциальную информацию, которую им не положено было знать;

- 82 % признались, что информацию, отображаемую на их экране, могли бы видеть посторонние лица;

- 82 % слабо уверены в том, что в их организации кто-либо будет защищать свой экран от посторонних лиц.

Применение техник социальной инженерии требует не только знания психологии, но и умения собирать о человеке необходимую информацию. Относительно новым способом получения такой информации стал её сбор из открытых источников, главным образом из социальных сетей. К примеру, такие сайты как livejournal, «Одноклассники», «ВКонтакте», «Instagram» содержат огромное количество данных, которые люди и не пытаются скрыть. Как правило, пользователи не уделяют должного внимания вопросам безопасности, оставляя в свободном доступе данные и сведения, которые могут быть использованы злоумышленником.

Таким образом, для обеспечения безопасности от методов социальной инженерии, надо скептически относится к любым подобным сообщениям. И для этого предлагаю некоторые принципы обеспечения безопасности:

-использование услуги определения номера;

-игнорирование неизвестных ссылок и смс-сообщении;

- обеспечение защиты информации о клиентах с помощью шифрования данных или использования управления доступом;

- обучение сотрудников навыкам для распознавания социального инженера;

- запрет персоналу обмен паролями либо использование общего;

Использованные источники:

1. Социальная инженерия, или Как «взломать» человека / [Электронный ресурс] – Режим доступа: https://www.kaspersky.ru/ (Дата обращения: 08.12.2017)

2. Социальная инженерия и социальные хакеры / [Электронный ресурс] – Режим доступа: https://kartaslov.ru/ (Дата обращения: 09.12.2017)

3. Социальная инженерия: хакерство без границ хакеры / [Электронный ресурс] – Режим доступа: https://www.livejournal.com/ (Дата обращения: 09.12.2017)