УДК 34.06

Шарыпова Т.Н.,
к.э.н., доцент кафедры информационных технологий
и защиты информации
Ростовский государственный экономический университет «РИНХ»
Россия, г. Ростов- на-Дону
Вяльцев Д.Р.,
студент 1 курс, факультет «Юриспруденция»
Ростовский государственный экономический университет «РИНХ»
Россия, г. Ростов- на- Дону

ПОЛУЧЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ С ПОМОЩЬЮ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ МЕТОДОМ «ДОРОЖНОЕ ЯБЛОКО»

Аннотация: *В данной статье представлена информация о том, как социальные инженеры заполучают конфиденциальную информацию своих жертв. Для этого используя один из самых простых и распространенных методов с названием «Дорожное яблоко». Этот способ основывается на том, что присуще каждому человеку – любопытство.*

Ключевые слова: *социальная инженерия, дорожное яблоко, взлом, информация, личные данные, киберпреступление.*

Abstract: *This article provides information about how social engineers get hold of their victims ' confidential information. To do this, using one of the simplest and most common methods called "Apple road". This method is based on the fact that inherent in every person – curiosity.*

Key words: *social engineering, apple road, hacking, information, personal data, cybercrime.*

Человек – это высший объект в психологической науке. Он не может существовать без взаимоотношений с другими людьми, так как является частью

социума. Человек, выполняя в обществе определённые социальные роли, занимает соответствующее место, получает свой социальный статус и доступ к ресурсам и благам, имеющимся в данном обществе.

С древних времен людей объединяли общие интересы, общие цели, ценности и традиции. Человек стремился окружить себя соплеменниками. Осознание себя, как отдельной личности заняло очень долгое время. До понимания своего «Я», появилось понимание «Мы». Человеку было очень сложно существовать обособленно от своего племени. Понимая, что ты один наедине с природой вселяло страх в людей. Недаром изгнание, на протяжении многих тысячелетий, являлось высшей мерой наказания.

Человек не может существовать вне социума, так как на подсознательном уровне нуждается во взаимоотношениях с другими людьми. Взаимоотношения, в свою очередь, строятся на общении, что даёт толчок к развитию индивида, как личности и общества в целом.

По сей день, неотъемлемой частью внутреннего мира человека, которое подталкивает на контакт с обществом, является доверие – важное, и в то же время, слабое место субъекта, как и любопытство. Проявлять интерес, стремиться знать, как можно больше, всегда волновало всех людей.

В поведении человека имеются систематические отклонения – когнитивные искажения, на которых основаны все техники социальной инженерии. Эти ошибки используются при атаке, с целью получения конфиденциальной информации, как правило, сама жертва, не подозревая этого, дает свое согласие. Человеческий фактор является одной из причин утечки персональных данных. [1]

Персональные данные – это любая личная информация гражданина, с помощью которой можно идентифицировать человека: фамилия, имя, отчество, место и год рождения, адрес прописки, паспортные данные и т.д.

Причинами утечки персональных данных, являются:

- потеря или кража оборудования, например, портативных компьютеров или телефонов, а также внешних носителей;

- взлом – одна из главных причин утечки персональных данных;
- заражение компьютера или телефона вредоносными программами;
- человеческий фактор, а именно доверчивость и любопытство человека, отвечать на e-mail рассылку, то есть спам. [2]

Социальная инженерия – это метод получения доступа к персональным данным, основываясь на психологии людей. Целью социальной инженерии является, получения доступа к конфиденциальной информации, паролям, банковским данным и другим защищённым системам, с помощью общения и психологического воздействия на жертву, добровольно, с её согласия.

В социальной инженерии много методов получения данных, таких как:

- фишинг – интернет-мошенничество, цель которого заполучить логин и пароль жертвы;
- телефонный фрикинг – взлом телефонных систем с целью получить бесплатные звонки;
- претекстинг – злоумышленник работает по заготовленному сценарию, где представляется другим человеком (сотрудником технической поддержки) и заполучает личную информацию. [3]

Еще один метод социальной инженерии является «Дорожное яблоко». Принцип использование данного метода на примере троянского коня. Суть его заключается в том, что злоумышленник, используя какой-либо носитель флэшу или жесткий диск, заражает его вредоносной программой – вирусом, оставляя в людном месте. Чаще всего, социальные инженеры оставляют такое портативное устройство в каких-либо компаниях. В таком случае указывается эмблема данной фирмы и делается незначительная, но в то же время броская надпись «данные по продажам», «график зарплаты», «отчёт в налоговую». Любопытный человек, сотрудник данной организации, либо непосредственно цель атаки решает принести этот носитель домой или на работу. Стоит только вставить носитель в компьютер, может обнаружиться, что накопитель пустой, но это только с первого взгляда. Тем не менее, вирус на нем есть, который, отныне, находится уже в вашем персональном компьютере. Это может быть обычным

кейлоггером – программа, которая фиксирует каждое нажатие клавиш на клавиатуре, каждый клик компьютерной мышки, сохраняет всю информацию в текстовом файле и отсылает злоумышленнику. В основном, эта программа используется вместе с вирусом, который очищает кэш вашего браузера, чтобы заставить вас заново ввести личные данные – логины и пароли. Именно за этой информацией и охотится социальный инженер, но так же вирус может быть гораздо серьезнее, чем кейлоггер - бэкдор (от англ. back door — «чёрный ход»). Эта программа делает компьютер полностью открытым для злоумышленника, что позволяет управлять вашим устройством на расстоянии, манипулировать данными и информацией. Это является очень большой проблемой, тем более, если вирусом поразили технику в какой-либо фирме, где, зачастую, все компьютеры соединены одной локальной сетью. Вся конфиденциальная информация может быть унесена в общий доступ или использоваться против вас самого. [4]

С увеличением популярности крипто-индустрии стали появляться и новые виды мошенничества, а точнее старые методы начали адаптироваться к новым реалиям. Только за прошедший год злоумышленникам удалось с помощью разных методов социальной инженерии совершить порядка 14 кибератак на криптовалютные биржи. Было украдено около $900 миллионов во всём мире, из них $7,5 миллионов приходится на Российскую Федерацию.

По логике, использование незнакомых носителей информации не очень хорошая идея, но человек по своей природе пытается узнать неизведанное.

Лишь в 3% случаях удаётся избежать внешнего вмешательства в персональный компьютер или телефон. Остальные 97% с огромным желанием решат проверить, что же есть на этом портативном устройстве. [5]

После того как флэшка или жёсткий диск будут использованы на компьютере, персональные данные мгновенно попадут в руки злоумышленников. Скорее всего, жертва не поймёт, что произошло, так как мошенникам нужно всего пару программ весом в несколько килобайт, чтобы

украсть все персональные данные которые имеются на персональном компьютере. [6]

Утечку персональных данных сложно определить. Возможно, украденная информация никогда не будет использована. По статистике киберпреступлений в Российской Федерации за 2018 год, мошенники украли только у финансовых организаций порядка $25 миллионов. По отчётам международной организации Group-IB, которая специализируется на предотвращение кибератак, злоумышленникам удалось обмануть граждан России на $8,3 миллиона, используя их персональные данные. Потерпевшие узнавали об этом через пару часов либо и вовсе не знали, что стали жертвами мошенничества

Таким образом, любопытство человека может сыграть против него самого. Нужно воздерживаться от желания использовать незнакомые портативные устройства, не отвечать на спам сообщения, не переходить по незнакомым ссылкам, не верить в лёгкий и быстрый выигрыш. Все эти схемы используют мошенники. Они давят на ваши самые слабые места: доброту, отзывчивость, доверие.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Васильев, М.В. Кибертерроризм как элемент гибридной войны. [Электронный ресурс]. – Режим доступа: https://www.geopolitica.ru/article/kiberterrorizm-kak-element-gibridnoy-voyny .

2. Мазуров, В.А Кибертерроризм: понятие, проблемы противодействия // Доклады ТУСУРа. – 2010. – №1 (21). - С. 41-45.

3. Шарыпова Т.Н., Свириденко А.А. Кибертерроризм – глобальная проблема современности. Научно-практический электронный журнал Аллея Науки. №1(28) 2019.

4. Шарыпова Т.Н., Сиваков В.Н. Киберпреступления. цели, последствия и методы защиты. Научно-практический электронный журнал Аллея Науки. №1(28) 2019.

5. Социальная инженерия и социальные хакеры / [Электронный ресурс] – Режим доступа: https://kartaslov.ru/

6. Социальная инженерия: хакерство без границ хакеры / [Электронный ресурс] – Режим доступа: https://www.livejournal.com/