Научная статья
Original article
УДК 343.9.01
DOI 10.55186/26584964_2022_5_6_1

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ КАК МЕТОД КИБЕРПРЕСТУПЛЕНИЯ

SOCIAL ENGINEERING AS A METHOD OF CYBERCRIME

Годунова Маргарита Сергеевна, студент кафедры «Современные технологии управления», МИРЭА – Российский технологический университет (РТУ МИРЭА), Москва, Россия
Копосова Мария Сергеевна, студент кафедры «Современные технологии управления», МИРЭА – Российский технологический университет (РТУ МИРЭА), Москва, Россия

Godunova Margarita Sergeevna, student of the Department of Modern Management Technologies, MIREA - Russian Technological University (RTU MIREA), Moscow, Russia
Koposova Maria Sergeevna, student of the Department of Modern Management Technologies, MIREA - Russian Technological University (RTU MIREA), Moscow, Russia

Аннотация: В современном мире человека окружает огромное количество опасностей, с совершенствованием цифровизации пришлось столкнуться с противоправными явлениями даже в информационно-телекоммуникационной среде. В данной статье рассмотрены теоретические

основы киберпреступлений, выделены основные техники и инструменты, раскрыта сущность самого популярного вида, с которым сложно бороться даже век цифровизации. Социальная инженерия наиболее распространённый способ заражения устройств и хищения личных данных. Противостоять данному виду киберпреступлений получается очень редко, но существуют базовые действия, которые стоит придерживаться, чтобы защитить себя.

S u m m a r y : In the modern world, a person is surrounded by a huge number of dangers, with the improvement of digitalization, illegal phenomena had to be faced even in the information and telecommunications environment. This article examines the theoretical foundations of cybercrime, highlights the main techniques and tools, reveals the essence of the most popular type, which is difficult to fight even in the age of digitalization. Social engineering is the most common way to infect devices and steal personal data. It is very rare to resist this type of cybercrime, but there are basic actions that should be followed to protect yourself.

Ключевые слова: киберпреступление, социальная инженерия, хакер, технологии, безопасность, манипуляция.

Keywords: cybercrime, social engineering, hacker, technology, security, manipulation.

В эпоху информационных технологий сложно представить жизнь без Интернета, люди всё больше и больше проводят там времени. Благодаря всемирной компьютерной сети появилась много возможностей, например, можно совершать покупки онлайн, общаться с друзьями, дистанционно учиться, работать и просто расслабляться после тяжелого дня. Проводя там много времени, люди оставляют огромное количество личных данных. Некоторые об этом задумываются и пытаются себя защитить, но обычный пользователь, не разбирающийся в IT-сфере, не сможет полностью оградиться от утечки данных.

Рост киберпреступлений - актуальная проблема, с которой становится трудно бороться с каждым днём. Данный вид мошенничества сложен в

раскрытии, правоохранительные органы нуждаются в кадрах с достаточно интеллектуальным потенциалом в сфере компьютерных технологиях [1].

Что же такое киберпреступления и как с ними бороться?

Это общее название для всех типов криминальной активности, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства. Известно, что киберпреступления не знают государственных границ, хакеры начали объединяться в целые организации, которые с лёгкостью взламывают базы данных, приложения, аккаунты в различных социальных сетях и даже получают доступ к секретной правительственной информации. Преступники «Всемирной паутины» используют личную информацию пользователей Интернета в своих корыстных целях.

Киберпреступления могут совершаться с помощью различных методов и инструментов, например, фишинг, вирусы, шпионское ПО, программы-вымогатели чаще всего используются с целью кражи личных данных или финансовых средств.

В данной работе будет раскрыт один из видов киберпреступлений, который по мнению учёных и IT-специалистов в скором времени будет представлять наибольшую угрозу информационной безопасности [4].

Социальная инженерия или «атака на человека» — это совокупность психологических и социологических приёмов, методов и технологий, которые позволяют получить конфиденциальную информацию. Другими словами, это манипулирование человеком с помощью использования социальных и психологических навыков без применения технических приёмов взломов для получения конфиденциальной информации [2].

Человек - существо социальное. Одно из основных и важнейших способностей является умение общаться с другими людьми. Довольно сложно представить свою жизнь в полном одиночестве, люди стремятся заводить друзей, окружать себя большим количеством знакомых. С детства родители закладывают ребёнку, что надо помогать окружающим, уважать старших и

быть честными по отношению друг к другу. Данные социальные тонкости подвергают нас опасности, из-за них люди стали слабым звеном в системе информационной безопасности [3].

В эпоху цифровизации технологии совершенствуются с каждым днём, а люди наоборот приобретают всё больше слабостей, предрассудков, которые мешают сохранять самообладание в стрессовых ситуациях. Даже самого внимательного и хладнокровного человека легко обмануть с помощью социальной инженерии, так как уже существует большой набор методов и инструментов данного вида киберпреступления (рисунок 1).



Источник: составлено автором

Рис. 1 – Распространённые техники социальной инженерии

Фишинг – самый популярный инструмент среди хакеров, так как это наиболее развитый вид мошенничества в Интернете. Ежедневно совершается более 135 миллионов фишинговых атак, каждое 2000 письмо является ловушкой [1].

Простыми словами, фишинг — это тактика рассылки мошеннических электронных писем и попытка обманом заставить получателей нажать на вредоносную ссылку или скачать зараженное вложение, с целью хищения

конфиденциальной информации. Письма приходят в виде рассылки от известных брендов, банков, социальных сетей, торговых компаний, возможны сообщения от лица собственной организации, например, от сотрудника из отдела кадров. Такие письма выглядят очень убедительно и не вызывают сомнений. Задача спам-сообщений – заставить человека перейти по вредоносной ссылке, после чего личные данные пользователя уже будут в руках мошенника [5].

Следующий вид социальной инженерии – претекстинг. Это атака, в которой злоумышленник представляется другим человеком и по заранее подготовленному сценарию узнает конфиденциальную информацию. Для успешного обмана мошенник должен обладать хоть какими-то данными о человеке, чтобы с помощью имеющихся деталей повысить к себе доверие жертвы.

Метод «Троянский конь» очень похож на фишинг, отличие в том, что это вредоносная программа, которую пользователь скачивает себе на устройство сам, а не просто кликает на ссылку [3].

Кви про кво используют, чтобы внедрить шпионское программное обеспечение в системы крупных организаций. Мошенники звонят в компанию, представляясь сотрудниками техподдержки, и проводят профилактические мероприятия на ПК. Работник организации делает всё сам, злоумышленники диктуют определённые команды, после чего появляется возможность запуска вирусного ПО [6].

Техника вишинг тоже является довольно популярной, она осуществляется с помощью телефонного звонка. Чаще всего мошенники звонят клиентам банков и пытаются выведать конфиденциальную информацию.

В основе метода «Дорожное яблоко» лежит «Троянский конь», отличие в том, что в первом случае используется физический носитель с вредоносным программным обеспечением. Социальные хакеры могут подбрасывать

загрузочные флешки или диски, подделанные под носители с интересным и уникальным контентом [5].

Обратная социальная инженерия является более трудоёмкой, чем обычная. Она требует особых знаний и навыков, но эффект от неё великолепный. Жертва по собственному желанию обращается к злоумышленнику и выдаёт все свои личные данные.

Социальная инженерия продумана до мелочей, с помощью данного вида киберпреступления мошенники наживаются довольно успешно. Но предостеречь себя от данных атак иногда возможно, следует выполнять следующие действия:

– не совершайте действий, если Вы полностью не уверены в их правильности;

– не переходите по сомнительным ссылкам из подозрительных источников;

– всегда перепроверяйте информацию, которую до вас пытается донести по телефонному разговору сотрудник какой-либо организации;

– используйте программы, которые будут предотвращать заражение устройств;

– не сообщайте никому свои личные данные.

Киберпреступления – это часть жизни современного человека, мошенники пытаются заработать любыми способами. Любой вид социальной инженерии всегда используется с плохим умыслом. Будьте бдительны, напоминайте своим близким и знакомым об элементарных правилах, которые не позволят попасться на крючок злоумышленников.

Литература

1. Кочкина, Э. Л. Определение понятия "киберпреступление". Отдельные виды киберпреступлений / Э. Л. Кочкина // Сибирские уголовно-процессуальные и криминалистические чтения. – 2017. – № 3(17). – С. 162-169.

2. Лыженкова, А. Н. Киберпреступления: понятие, классификация, юридическая ответственность, основные правила компьютерной безопасности / А. Н. Лыженкова, Т. Н. Шарыпова // Инновации. Наука. Образование. – 2021. – № 26. – С. 900-904.
3. Новопавловский, А. А. Социальная инженерия и конструирование «несовершенного пользователя» в кибербезопасности / А. А. Новопавловский, К. Верейкин // Угрозы и риски финансовой безопасности в контексте цифровой трансформации: Материалы VII Международной научно-практической конференции Международного сетевого института в сфере ПОД/ФТ, Москва, 24 ноября 2021 года. – Москва: Национальный исследовательский ядерный университет "МИФИ", 2021. – С. 709-718.
4. Семенов, М. Ю. Мошенничество в сети Интернет: отношение молодежи / М. Ю. Семенов, П. В. Качанова // Вестник Тюменского государственного университета. Социально-экономические и правовые исследования. – 2021. – Т. 7. – № 3(27). – С. 71-85.
5. Филин, Е. А. Подследственность и подсудность киберпреступлений / Е. А. Филин // Уголовный процесс. – 2021. – № 11(203). – С. 72-77.
6. Янгаева, М. О. Социальная инженерия как способ совершения киберпреступлений / М. О. Янгаева // Вестник Сибирского юридического института МВД России. – 2021. – № 1(42). – С. 133-138.

Literature

1. Kochkina, E. L. Definition of the concept of "cybercrime". Certain types of cybercrimes / E. L. Kochkina // Siberian criminal procedural and criminalistic readings. – 2017. – № 3(17). – P. 162-169.
2. Lyzhenkova, A. N. Cybercrime: concept, classification, legal responsibility, basic rules of computer security / A. N. Lyzhenkova, T. N. Sharypova // Innovation. The science. Education. – 2021. – No. 26. – P. 900-904.
3. Novopavlovsky, A. A. Social engineering and the construction of an "imperfect user" in cybersecurity / A. A. Novopavlovsky, K. Vereykin // Threats and risks

of financial security in the context of digital transformation: Proceedings of the VII International Scientific and Practical Conference of the International Network Institute in the Field of AML/CFT, Moscow, November 24, 2021. – Moscow: National Research Nuclear University "MEPhI", 2021. – P. 709-718.

4. Semenov, M. Yu. Fraud on the Internet: the attitude of youth / M. Yu. Semenov, P. V. Kachanova // Bulletin of the Tyumen State University. Socio-economic and legal studies. – 2021. – T. 7. – № 3(27). – P. 71-85.
5. Filin, E. A. Investigation and jurisdiction of cybercrimes / E. A. Filin // Criminal process. – 2021. – № 11(203). – P. 72-77.
6. Yangaeva, M. O. Social engineering as a way of committing cybercrimes / M. O. Yangaeva // Bulletin of the Siberian Law Institute of the Ministry of Internal Affairs of Russia. – 2021. – № 1(42). – P. 133-138.

© Годунова М.С., Копосова М.С. 2022 Научно-образовательный журнал для студентов и преподавателей «StudNet» №6/2022.

Для цитирования: Годунова М.С., Копосова М.С. СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ КАК МЕТОД КИБЕРПРЕСТУПЛЕНИЯ// Научно-образовательный журнал для студентов и преподавателей «StudNet» №6/2022.