ПРИМЕНЕНИЕ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ В СОЦИАЛЬНЫХ СЕТЯХ

ДЬЯКОВ Никита Владимирович
ФГБОУ ВО «Донской технический государственный университет»
г. Ростов-на-Дону, Россия

В данной статье приводится одна из главных проблем современного общества – мошенничество в интернете, а в частности, в социальных сетях. В статье рассмотрены виды и формы социальной инженерии. Приведен анализ различных способов мошенничества в социальных сетях, такие как взлом страниц, переход по ссылке, отправка зараженных файлов и т. д. Особое внимание уделяется социальной инженерии и факторам, благодаря которым злоумышленники получают доступ к персональным данным своих жертв. По результатам исследования созданы свод правил безопасности для пользователей социальных сетей.

Ключевые слова: социальная инженерия, социальные сети, мошенничество, глобальная сеть, уязвимость.

Информация представляет собой один из наиболее важных ресурсов современного общества, поэтому обеспечение комплексной защиты информации является одной из важных и приоритетных задач в информационной безопасности. С каждым годом информационные системы защиты совершенствуются в связи с постоянным развитием современных технологий. Информационные системы защиты могут продолжительное время функционировать в заданных пределах и решать поставленные задачи, что нельзя сказать о самом человеке. Люди, так и будут оставаться основной уязвимостью, со своими слабостями, предрассудками, являясь наиболее слабым звеном в цепочке информационной безопасности. Глобальная сеть, как основной и самый быстрый источник получения и распространения информационных ресурсов, таит в себе немало угроз [1]. Она стремительно разрастается и с каждым днём все больше и больше внедряется в различные сферы человеческой жизни.

Мошенничество в социальных сетях. Понятие, как мошенничество, на сегодняшний день, очень распространенное. С законодательной точки зрения, мошенничество представляет собой хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием (статья 159 УК РФ) [2]. На сегодняшний день в России мошенничество распространено довольно широко и оно очень разнообразно. Можно сказать, стало массовым явлением.

Уголовный кодекс определяет способы мошенничества, которые заключаются в хищении чужого имущества или приобретении права на чужое имущество одним из двух указанных в нем способов: обман и злоупотребление доверием.

Основная часть видов мошенничества известна уже многие времена. Они могут быть самыми разнообразными. Традиционные виды мошенничества [2]:

– в сфере кредитования;
– при получении выплат;
– с использованием платежных карт;
– в сфере страхование и др.

Мошенничество в глобальной сети, представляет собой самую незащищенную сферу социально-общественных отношений. Вычислить преступников очень сложно, практически невозможно: отсутствует доказательная база по различным видам преступлений в сети. В УК РФ в принципе отсутствует норма, которая могла бы регулировать социально-общественные отношения в Глобальной сети, а, следовательно, предусматривать ответственность за совершение преступных деяний в ней.

АУДИТОРИЯ СОЦИАЛЬНЫХ СЕТЕЙ ЗА НОЯБРЬ 2019 [3]

	Инстаграм	Вконтакте	Фейсбук	Одноклассники	YouTube
Кол-во людей, заходивших хотя бы 1 раз	33598	40108	23864	25852	45531
Ср. кол-во минут 1 поль-ля в день	26 мин	36 мин	8 мин	22 мин	47 мин

Основная часть мошенников нацелена на получение денежных средств. Самые распространенные способы [4]:

– взлом страницы в социальной сети, с целью шантажа или смс с просьбой прислать деньги;

– собирание денег на помощь, например, кто-то попал в больницу и нужны деньги на операцию;

– переход по ссылке;

– отправка зараженных файлов;

– фишинг;

– получение предоплаты за покупку товара;

– вредоносные сервисы, программы и т. д.;

– предложение «легкого» дополнительного заработка.

Но есть моменты, когда мошенников в социальных сетях не интересует финансовая сторона вопроса. Например, мошенники в социальных сетях могут преследовать такие цели, как:

– рассылка спама;

– реклама;

– кража персональных данных.

Таким образом, самое уязвимое место в защите информационной системе от мошенничества это человек. Никакие программно-аппаратные средства не защитят вас, если вы будете неосторожны и невнимательны.

Основные факторы, благодаря которым, социальная инженерия имеет возможность быть [5]:

1. Жажда легкой прибыли.

2. Страх, например, «Пройдите по ссылке, иначе ваш аккаунт будет заблокирован!».

3. Наивность, легковерность.

4. Любопытство.

Для того чтобы обезопасить себя при работе в глобальной сети и при использовании социальных сетей, любой пользователь должен соблюдать несколько правил:

– не оставляйте свои персональные данные на открытых ресурсах;

– не откликайтесь на заманчивые предложения;

– при получении сообщения о блокировке аккаунта не вводите данные во вложенные формы;

– сравните адрес, с которого пришло письмо, с адресом, с которого приходили сообщения от сети ранее;

– после загрузки страницы, обязательно проверьте наличие защищенного соединения;

– если вы стали получать подозрительные письма и сообщения от ваших друзей, постарайтесь связаться с ними другим способом.

СПИСОК ЛИТЕРАТУРЫ

1. ЯКЛАСС. Глобальная сеть Интернет. Общая характеристика, особенности построения инженерия. – URL: https://www.yaklass.ru/materiali?mode=cht&chtid=464/ (дата обращения: 01.03.2020).

2. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 18.02.2020) // Мошенничество, 08.12.2003, N 162-ФЗ, статья 159.

3. Статистика социальных сетей в России 2019. – URL: https://livedune.ru/blog/statistika_socsetej_v_rossii/ (дата обращения: 01.03.2020).
4. *Аюпова К.В., Аюпов Р.Ш.* Социальная инженерия – современная угроза информационной безопасности // Актуальные проблемы и перспективы инновационного развития современной России. – 2014. – С. 125-128.
5. *Комаров А.А.* Интернет-мошенничество: проблемы детерминации и предупреждения // Сер. Криминология / монография. Москва, 2013.

APPLICATION OF SOCIAL ENGINEERING METHODS IN SOCIAL NETWORKS

DYAKOV Nikita Vladimirovich
Don Technical State University
Rostov-on-Don, Russia

This article presents one of the main problems of modern society - fraud on the Internet, and in particular on social networks. The article considers the types and forms of social engineering. The analysis of various methods of fraud on social networks, such as hacking pages, clicking on the link, sending infected files, etc. is given. Particular attention is paid to social engineering and the factors due to which attackers gain access to the personal data of their victims. Based on the results of the study, a set of safety rules for users of social networks has been created.
Key words: social engineering, social networks, fraud, global network, vulnerability.