УДК 004.056

ОСНОВНЫЕ УГРОЗЫ В ИНТЕРНЕТЕ И СПОСОБЫ ИХ ПРЕДОТВРАЩЕНИЯ

Ю. А. Кравченко, К. А. Пыханов
Донской государственный технический университет (г. Ростов-на-Дону, Российская Федерация)

Аннотация. Сегодня человек не представляет свою повседневную жизнь без компьютера, ноутбука, телефона, планшета, с помощью которых он может выйти в Интернет, получить любую интересующую его информацию. Современное общество так и называют — информационным. Интернет плотно вошел в нашу жизнь, мало кто из его пользователей не зарегистрирован ни в одной из социальных сетей. Но кроме получения полезной информации, возможности общения, социальные сети могут принести пользователю различного рода угрозы. Цель авторов данной статьи — проанализировать эти угрозы, определить возможности их избежать или предотвратить. Актуальность проблемы информационной безопасности в социальных сетях заключается в том, что с развитием таких сетей их пользователи сталкиваются с новыми интернет-технологиями, в которых не всегда предусмотрена система информационной безопасности

Ключевые слова: информационная безопасность, общество, социальные сети, персональные данные, конфиденциальность данных, информационные технологии, система, Интернет.

MAIN THREATS ON THE INTERNET AND WAYS TO PREVENT THEM

Yuliya A. Kravchenko, Kirill A. Pykhanov
Don State Technical University (Rostov-on-Don, Russian Federation)

Abstract. Today, a person cannot imagine his daily life without a computer, laptop, phone, tablet, with which he can access the Internet, get any information he is interested in. Modern society is called information society. The Internet has firmly entered our lives. Only few of its users are not registered in any of the social networks. But in addition to obtaining useful information, communication opportunities, social networks can bring various kinds of threats to the user. The authors' objective is to analyze these threats, determine the possibilities to avoid or prevent them. The relevance of the problem of information security in social networks lies in the fact that with the development of such networks, their users face new Internet technologies that do not always provide an information security system.

Keywords: information security, society, social networks, personal data, data privacy, information technology, system, Internet.

Введение. Социальная сеть — это платформа, которая используется для общения, знакомств, обмена информацией, ресурс можно использовать и в качестве развлечения: здесь есть музыка, книги, фильмы. Человек может придумать себе любой образ для общения или реализации своей личности, выкладывать информацию про себя, свои интересы. Но чем больше персональной информации попадает в сеть, тем тщательнее пользователю нужно следить за безопасностью своего аккаунта, так как любой злоумышленник может воспользоваться его личными данными [1]. Проблема безопасности персональных данных актуальна на протяжении уже длительного времени, так как не один год используются интернет-ресурсы. Поэтому помнить о защите персональных данных нужно постоянно.

Основная часть. Информация, содержащаяся в соцсетях, очень часто становится объектом незаконных действий мошенников, специализирующихся на кражах персональных данных,

которые могут быть использованы для аутентификации на различных ресурсах и сайтах.

Основные угрозы, которые встречаются в сети Интернет:

1. Фишинг. Это самый распространенный вид угрозы, представляющий собой противозаконное действие, направленное на получение конфиденциальной информации пользователя, которая потом используется с целью кражи денежных средств или для продажи на черном рынке. Чаще всего злоумышленники отправляют потенциальной жертве электронное или текстовое письмо от какого-либо лица или организации (например от друга или сотрудника банка) и просят перейти по указанной ими ссылке, где для просмотра того или иного контента требуется авторизоваться на сайте, который имитирует официальный информационный ресурс, таким образом введенные пострадавшим данные попадающие в руки похитителя.

2. Вредоносные программы. Данный вид угрозы по частоте использования злоумышленниками стоит наравне с фишингом. Пользователи скачивают в Интернете приложения и игры как с официальных, так и с неофициальных сайтов. Последний вариант очень опасен, так как нарушители нередко выгружают в Интернет зараженный контент, после установки которого на компьютер жертвы вместе со скаченным приложением заносятся компьютерные вирусы, троянцы или черви, которые приносят вред самому компьютеру, сетям и данным пользователя.

3. DoS и DDoS атаки. Такие атаки не предназначены для кражи информации или для нанесения вреда системе, их цель направлена на самое важное — на доступность к определенному ресурсу информации, например Web-сайт или приложение. DoS — это атака, которая идет от одного источника, она отправляет множество пакетов и запросов на сервер, что ведет к его перегрузке. DDoS — это разновидность DoS-атаки, где используется не один источник, а несколько, например аккаунты, которые куплены, были взломаны злоумышленником или которыми владеет он сам. Все это используется для борьбы с конкурентами, с целью вымогательства, хактивизма или по причине личной неприязни.

Для предотвращения или минимизации таких угроз существует система информационной безопасности. Ее цель — совершенствование и поддержка работоспособности системы, сохранение конфиденциальной информации пользователя и самой системы, сведение к минимуму количества нарушений в ее работе, происходящих как от естественных, так и от преднамеренных угроз [2].

Целью системы информационной безопасности принято считать:

– улучшение безопасности;

– поддержании безопасности;

– сведение к минимуму нарушений в системе (не только от естественных, но и от преднамеренных угроз);

– предотвращение вторжений;

– уничтожение нарушений в случае вторжений.

Если рассматривать информационную безопасность на государственном уровне, то в Российской Федерации это понимается как состояние защищенности ее национальных интересов в информационной сфере, которая включает в себя интересы личности, общества в целом и государства.

Можно выделить главные принципы информационной безопасности для социальных сетей:

1. Доступность. Пользователь должен быть уверен в надежности и эффективности получаемой информации, а также в том, что доступ к ней будет только у проверенных лиц. В случае вторжения гарантируется восстановление без потери данных.

2. Целостность. Это комплексные действия при защите информации, которые обеспечат работоспособность системы без каких-либо неполадок.

3. Конфиденциальность. Конфиденциальная информация — информация, за которой нужно тщательно следить, чтобы не было ее утечки, чтобы мошенники не могли ею воспользоваться. Конфиденциальность должна присутствовать на всех этапах разработки системы информационной безопасности.

Чтобы избежать вторжения в свои социальные сети и обезопасить себя и свои личные данные, необходимо соблюдать следующие правила:

1. Самое важное и главное — это пароль. Пароль должен быть сложный, так как злоумышленники сталкиваются с ним в первую очередь. Для каждой социальной сети нужен собственный пароль, чтобы обеспечить надежность. Да, большое количество паролей запомнить трудно, но, если он будет одинаковым для всех соцсетей, то, узнав пароль от одной, правонарушитель получит доступ ко всем страницам. Также пароль не должен содержать личные данные пользователя: дату рождения, место рождения, место пребывания, имя, фамилию — такие пароли не надежны.

2. Электронная почта. Необходимо иметь отдельную почту для привязки к странницам, например, если использовать рабочую почту, в случае взлома злоумышленник получит доступ к конфиденциальным данным, а если использовать личную почту, то к личным данным.

3. В социальные сети желательно выкладывать небольшой объем информации. Допустим, можно выложить фото, но без рассказа о личной жизни, распорядке дня, месте положения.

4. Необходимо настроить восстановление пароля и периодически его обновлять. Самый простой и надежный способ — это номер телефона, так как гаджет часто находится рядом с владельцем, и будет трудно узнать код, приходящий на номер телефона. Не надежно будет привязывать вторую электронную почту или секретное слово.

5. Следует ознакомиться с политикой конфиденциальности социальной сети перед внесением личных данных, чтобы увидеть, какая информация будет видна посторонним лицам.

6. Необходимо просматривать и подключать дополнительные функции, которые может предоставить владелец социальной сети для безопасности аккаунта.

7. Не распространять через личные сообщения документы и конфиденциальную информацию.

8. Не выкладывать фотографии документов в социальных сетях.

Заключение. В данной статье были рассмотрены некоторые виды угроз, с которыми могут столкнуться пользователи сети Интернет. Предложены рекомендации для их предотвращения, это и сложный пароль, и особая осторожность при входе в соцсети, и сокращение выкладываемой в сеть информации. В современных социальных сетях предпринимаются различные меры для защиты персональных данных, для того, чтобы информация пользователей не стала общедоступной. Но при этом авторы отмечают, что человек должен и сам понимать, какую информацию можно выкладывать в сеть, а какую нельзя. Однако, если будут соблюдены все вышеуказанные меры безопасности, риск кражи персональных данных уменьшится до минимума.

Библиографический список

1. Буянов, Д. С. Информационная безопасность в социальных сетях / Д. С. Буянов // Молодой ученый : [сайт]. — 2018. — № 39 (225). — С. 14–16. — URL: https://moluch.ru/archive/225/52820/ (дата обращения: 10.12.2022).

2. Обеспечение безопасности системы информационно-аналитической поддержки научных исследований / Е. В. Чернова, Е. В. Попова, И. В. Попова, И. В. Зленко // Программные продукты и системы. — 2009. — № 4. — С. 48–50.

Об авторах:

Кравченко Юлия Андреевна, студентка кафедры «Вычислительные системы и информационная безопасность» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), yuliakravchenkooo@gmail.com

Пыханов Кирилл Андреевич, студент кафедры «Вычислительные системы и информационная безопасность» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), lirik200229@gmail.com

About the Authors:

Kravchenko, Yuliya A., student of the Computing Systems and Information Security Department, Don State Technical University (1, Gagarin sq., Rostov-on-Don, 344003, RF), yuliakravchenkooo@gmail.com

Pykhanov, Kirill A., student of the Computing Systems and Information Security Department, Don State Technical University (1, Gagarin sq., Rostov-on-Don, 344003, RF), lirik200229@gmail.com