УДК 004

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОЦИАЛЬНЫХ СЕТЯХ

Журавлева В.В.,

студент,

Калужский государственный университет им. К.Э.

Циолковского,

Калуга, Россия

Ткаченко А.Л.,

к.т.н., доцент,

Калужский государственный университет им. К.Э.

Циолковского,

Калуга, Россия

Аннотация. Пользователи Интернета подвергаются множеству опасностей в сети, даже не подозревая об этом. Важно предупредить атаки мошенников и обеспечить защиту собственных данных. В данной статье рассматривается проблема информационной безопасности в социальных сетях, а именно каким образом данные оказываются в руках мошенников и как противостоять перехвату конфиденциальной информации пользователя в сети Интернет.

Ключевые слова: фишинг, социальная инженерия, дэйтинг-мошенничество, информационная безопасность, мошенничество.

INFORMATION SECURITY IN SOCIAL NETWORKS

Zhuravleva V.V.,

student,

Kaluga State University named after K.E. Tsiolkovsky,

Kaluga, Russia

Tkachenko A.L.,

Candidate of Technical Sciences, Associate Professor,

Kaluga State University named after K.E. Tsiolkovsky,

Kaluga, Russia

Annotation. Internet users are exposed to many dangers online without even knowing it. It is important to prevent fraud attacks and ensure the protection of your own data. This article discusses the problem of information security in social networks, namely, how data ends up in the hands of fraudsters and how to resist the interception of confidential user information on the Internet.

Keywords: phishing, social engineering, dating fraud, information security, fraud.

Появление социальных сетей, а со временем и способность с помощью сервисов совершать различные действия с занесением личных данных в Интернете, привело к распространению мошенничества. Основной причиной утечки информации о пользователе происходит из-за неопытного обращения с социальными сетями, а также полное игнорирование систем защиты персональных данных. В большинстве своем общество и не представляет, что данные могут быть похищены и использованы против них [1, 2]. Интернет-мошенничество является одной из самых распространённых проблем современного мира. Хотя борьба с преступностью в социальных сетях поэтапно решается, все же вместе с развитием технологий модернизируются и способы перехвата личных данных в криминальных целях.

С появлением коммерческого Интернета в 1990-х годах участились случаи хищения данных кредитных карт и паспортных данных. И со временем эти случаи стали обыденными в сети. В особенности о безопасности информации

заботятся крупные компании и государственные организации [3-5]. Но без актуальных систем защиты мошенники смогут взломать систему и похитить важные данные. В области информационной безопасности в компании «РТК-Солар» были выявлены 325 000 угроз ко второму кварталу 2023 года, что превышает показатели прошлого года на 38%.

Существуют законы, за счет которых защищаются интересы личности, а именно его неприкосновенность, личная жизнь, защита чести и имени. Например: статья 23 Конституции Российской Федерации определяет право человека на конфиденциальность своей личности. Но далеко не каждого мошенника удается вычислить, так как они используют хорошую систему защиты информации о своем местонахождении.

В современном мире есть множество видов угроз информационной безопасности. Общество может столкнуться с такими видами кибератак как:

1) Фишинг. Это один из самых распространенных способов обмана в Интернете. Он скрывается в рассылках электронных писем под видом сторонних ссылок. Характерно для данного вида атак то, что мошенникам становиться известна вся информация, введенная пользователем на сервисе по ссылке, а именно логин и пароль, по которым взламываются социальные сети. Такого вида кибератаки непредсказуемы, и даже опытные пользователи не смогут различить угрозу.

2) Нередко злоумышленники выдают себя за специалистов из банка или других служб, чтобы убедить человека переслать личные данные для якобы предотвращения хищения денежных средств. Такая схема называется социальная инженерия. Она достаточно популярна, особенно среди пенсионеров. Дэйтинг-мошенничество также использует эмоциональную манипуляцию, но в данном случае люди скрываются под видом ложных личностей.

3) В некоторых ситуациях людей заставляют вложить деньги в

инвестиции для получения большой прибыли. Ложная реклама и обманчивая схема направляют жертву в ловушку.

Это далеко не полный список кибератак, которые преследуют людей повсеместно. Все угрозы становятся сложнее и адаптируются к поведению людей [6].

Чтобы позаботиться о безопасности данных в Интернете необходимо придерживаться определенных правил.

1. Для регистрации в социальных сетях требуется электронная почта. Не рекомендуется использовать почту, в которой хранится информация о данных банковских карт.
2. Как показывает практика многие используют один пароль для нескольких сервисов, но даже несмотря на его сложность это опасно. При взломе одного сервиса можно взломать таким же паролем и все остальные. Так же пароль необходимо периодически менять и обеспечить его восстановление в случае утери. Как способ подтверждения или восстановления лучше всего использовать телефон, так как физически им владеет только пользователь.
3. Быть внимательным при переходе на посторонние ссылки.
4. Не рекомендуется использовать социальные сети на рабочем месте. Попадание вирусов на рабочий компьютер может повлиять на корпоративную сеть в целом.
5. Всегда использовать антивирус и не устанавливать посторонние программы на компьютер с неизвестных сервисов.

Пользователи социальных сетей должны помнить, что существует риск попадания опубликованной информации в руки злоумышленника и вследствие чего данные будут использованы против человека. Следует помнить, что использование любого из средств защиты не даст гарантии, что персональные данные будут в безопасности. Но если соблюдать правила хранения данных и поведения в Интернете удастся снизить риск кражи личной информации.

Библиографический список:

1. Ибрагимова, З. М. Информационная безопасность как элемент экономической безопасности / З. М. Ибрагимова, З. Б. Батчаева, А. Л. Ткаченко // Инженерный вестник Дона. – 2022. – № 11(95). – С. 26-33. – EDN AMZDZG.
2. Чаусов, Н. Ю. Информационное обеспечение управления в it-организации / Н. Ю. Чаусов, Д. В. Короходкин // Вектор экономики. – 2022. – № 11(77). – DOI 10.51691/2500-3666_2022_11_7. – EDN ODRGWL.
3. Малюкова, Д. С. Информационные технологии в биомедицине и генетике / Д. С. Малюкова, А. Л. Ткаченко, А. В. Мазин // Modern Economy Success. – 2022. – № 1. – С. 53-57. – EDN MYAWRG.
4. Ткаченко, А. Л. Реинжиниринг бизнес-процессов туристической компании / А. Л. Ткаченко, А. А. Щеглова // Вестник Калужского университета. – 2021. – № 1(50). – С. 77-80. – EDN AMWKWN.
5. Экономическая безопасность РФ и Республики Беларусь в условиях новых западных санкций: поиск конструктивных решений / А. А. Мигел, А. А. Антонова, Д. А. Кокорев, Н. Д. Степин // Вестник Академии знаний. – 2023. – № 4(57). – С. 187-190. – EDN BQSQLN.
6. Кондрашова, Н. Г. Обеспечение экологической безопасности предприятия: экономический механизм / Н. Г. Кондрашова, Е. А. Рябой // Международный журнал гуманитарных и естественных наук. – 2022. – № 12-3(75). – С. 102-105. – DOI 10.24412/2500-1000-2022-12-3-102-105. – EDN BGQRPU.

Оригинальность 84%