УДК 343.72

МОШЕННИЧЕСТВО ЧЕРЕЗ МЕССЕНДЖЕР «ТЕЛЕГРАМ»

Н. Н. Коваленко
курсант 2 курса
Карагандинской академии МВД Республики Казахстан
имени Баримбека Бейсенова
Научный руководитель: ***М. Е. Кашенов****,*
преподаватель кафедры криминалистики
Карагандинской академии МВД Республики Казахстан
имени Баримбека Бейсенова

За все время существования человечества в нем всегда находили место уголовные правонарушения, связанные с мошенничеством. В эпоху цифровизации в связи с технологическим прорывом проблема мошенничества вышла на новый уровень — интернет-мошенничество. В Казахстане мошенничество квалифицируется в ст. 190 Уголовного кодекса Республики Казахстан от 3 июля 2014 года как «хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотреблением доверием» [1; 2].

Актуальность борьбы с интернет-мошенничеством в социальных сетях и мессенджерах проявляется в том, что люди всех возрастов пользуются ими и даже не догадываются, что их конфиденциальная информация и банковские счета могут быть использованы злоумышленниками.

Рассмотрим современные способы мошенничества в мессенджере «Телеграм» и способы защиты и борьбы с ними.

Основные способы интернет-афер через мессенджер «Телеграм»:

1) различные фишинговые ссылки;
2) получение личной информации через канал «Избранное»;
3) создание канала от имени юридических лиц с компетентными вакансиями;
4) продажа ответов по государственным экзаменам школьникам или студентам;
5) кардинг [3].

Предлагаем разобрать каждый из этих способов более детально.

1. Фишинг — это получение паролей и конфиденциальной информации, при котором в телеграм-каналах публикуется ссылка, при переходе по которой требуется авторизация. Появляется окно, в котором требуется заполнить личные данные и подтвердить их с помощью SMS-кода. После подтверждения через SMS аккаунт блокируют и в дальнейшем требуют денежную сумму за возврат аккаунта.

Для защиты от данного преступления требуется прежде всего бдительность лиц при использовании мессенджера. Двухфакторная аутентификация, конечно, не обеспечит полной защиты, однако затруднит действия мошенников. Необходимо обращать внимание на доменное имя ссылки. Если запрос идет от учетной записи телеграм, то должны присутствовать подтверждающие знаки в виде многогранника с галочкой внутри.

2. Канал «Избранное» — это системная группа в мессенджере «Телеграм», которую используют для хранения личной информации, в которой также могут быть сведения о счетах, номерах и т. д.

Мошенники создают канал с названием «Избранное», устанавливают аватар как на подлинном канале и добавляются на страницу.

Как понять, что это поддельный канал? Во-первых, в системной группе никогда не будет отображаться значок активности онлайн. Во-вторых, при создании данной группы она будет размещена сверху вашего чата некоторое время, так как мошенники будут писать сообщения и удалять их. Это делается для того, чтобы подлинный канал «Избранное» был скрыт внизу чата.

Для защиты требуется внимательность владельцев мессенджера.

3. Многие мошенники создают канал от имени какого-либо юридического лица, через который принимают документы для трудоустройства, тем самым получают сведения, через которые могут оформить кредит или совершить иную сделку с банком.

Для защиты требуется знать следующее:

1) юридические лица никогда не принимают на работу без собеседования;

2) через мессенджеры они ведут лишь распространение информации об имеющихся у них вакансиях, а не набор;

3) осуществлять набор они могут лишь со своих официальных сайтов.

4. Продажа ответов по государственным экзаменам школьникам или студентам. Мошенники пользуются морально-психологическим состоянием обучающихся перед экзаменами и предлагают приобрести ответы, при этом ответы либо не совпадают, либо отсутствуют.

Во избежание мошенничества данного типа требуется знать следующее: ответы на государственные экзамены имеются только в Министерстве образования, причем вопросы обновляются 1 раз в квартал [4; 5].

5. Кардинг — это современный вид мошенничества, основанный на использовании карты без участия ее законного владельца. Проще говоря, это обналичивание денег с помощью банковских карт. Злоумышленник, имея данные карты (номер карты, срок действия, CVV-код), может воспользоваться денежными средствами различными методами. Поэтому в Телеграме мошенники создают каналы от имени банка или каналы о предоставлении услуг.

Чтобы защитить свои персональные данные, требуется знать следующее:

1) данные банковских карт являются конфиденциальными и не подлежат разглашению третьим лицам; категорически запрещается фиксация кредитных и банковских карт с обеих сторон;

2) в случае утери или передачи данных карты следует немедленно обратиться в банк для ее блокировки [6].

Данный перечень способов мошенничества в мессенджере «Телеграм» не является исчерпывающим. Каждый день создаются новые изощренные способы обмана, поэтому для решения данной проблемы предлагаем следующее:

1. Проводить профилактическую работу не только с лицами подросткового и студенческого возраста, но и с лицами преклонного возраста, так как чаще всего именно они являются объектами мошенничества.

2. Создать горячую линию, например, 102*4, которая будет круглосуточно осуществлять помощь лицам, пострадавших от атак интернет-мошенников.

3. Создать специальную группу по мониторингу и пресечению противозаконных деяний мошенников в сети Интернет, при этом данная группа должна составлять определенную структуру. Например, направление по борьбе с мошенниками в социальных сетях и мессенджерах, направление по борьбе с сайтами-фальшивками и другое.

4. Внести изменения в Уголовные и Уголовно-процессуальные кодексы стран СНГ с учетом новых видов мошенничества и способов их расследования. К примеру, в Уголовный кодекс Республики Казахстан можно добавить дополнительную статью 190-1 (Мошенничество в сети).

---

1. Рассел Дж. Мобильное мошенничество. М. : VSD, 2013. 728 с. Вернуться к статье

2. Уголовный кодекс Республики Казахстан [Электронный ресурс] : 3 июля 2014 г., № 226-V ЗРК. Доступ из информационно-правовой системы «Әділет». Вернуться к статье

3. Гладкий А. Мошенничество в Интернете. Методы удаленного выманивания денег, и как не стать жертвой злоумышленников. М. : АВТОР, 2012. 589 с. Вернуться к статье

4. Как не стать жертвой преступления, мошенничества и обмана. М. : Текарт, 1995. 288 с. Вернуться к статье

5. Шейнов В. П. Как защититься от обмана и мошенничества : моногр. М. : Харвест, 2004. 464 с. Вернуться к статье

6. Хакимова Г. Мошенничество в сфере банковского кредитования. М. : Lambert Academic Publishing, 2022. 126 с. Вернуться к статье