УДК 338.2.

СПОСОБЫ ПРОТИВОДЕЙСТВИЯ ТЕЛЕФОННЫМ МОШЕННИКАМ В БАНКОВСКОЙ СФЕРЕ

***Мурзакова С.М.*[1],**
студент,
ФГБОУ ВО «Елецкий государственный университет им. И.А. Бунина»,
Елец, Россия

Аннотация.
В этой статье рассмотрены наиболее популярные способы мошеннических действий, осуществляемых с использованием средств мобильной коммуникации и электронных способов перевода денежных средств. Представлены известные методы различных банков по обеспечению безопасности своих клиентов от совершения «доверительных» переводов.

Ключевые слова: мошенничество, банк, безопасность, электронные переводы, страхование, кредитные учреждения.

WAYS TO COUNTERACT TELEPHONE FRAUD IN THE BANKING SECTOR

***Murzakova S.M.*[2],**
student
Bunin Yelets State University
Yelets, Russia

[1] *Научный руководитель – **Степаненкова Н.М.,** к.э.н., доцент, ФГБОУ ВО «Елецкий государственный университет им. И.А. Бунина», Елец, Россия*

[2] ***Stepanenkova N.M.,** PhD, Associate Professor, Bunin Yelets State University, Yelets, Russia*

Abstract

This article discusses the most popular methods of fraudulent activities carried out using mobile communication tools and electronic money transfer methods. The well-known methods of various banks to ensure the safety of their customers from making "trust" transfers are presented.

Keywords: fraud, bank, security, electronic transfers, insurance, credit institutions.

Использование современных технологий коммуникации побуждает к развитию не только новых форм общения между людьми на расстоянии, но и преступной деятельности с их применением. В условиях новых тенденций мошенники сталкиваются с меньшим риском, адаптируя под свои цели современные технологии. В итоге, чтобы получить денежные средства другого человека, стоит освоить минимальные навыки пользователя мобильных устройств. Ключевую роль играют манипуляции, которые придумывают с целью убеждения жертвы в переводе денежных средств.

Мошенничество, указанное в статье 159 УК РФ, является преступлением против собственности и предусматривает уголовную ответственность за хищение, совершенное путем обмана или злоупотребления доверием. Уголовный кодекс содержит общее понятие мошенничества, закрепленное в статье 159, и еще несколько специальных норм, таких как 159.1 - мошенничество в сфере кредитования, 159.2 - мошенничество при получении выплат, 159.3 - мошенничество с использованием электронных средств платежа, 159.5 - мошенничество в сфере страхования, 159.6 – мошенничество в сфере компьютерной информации.

Основные инструменты, используемые на мобильном устройстве с целью совершения мошеннических действий:

- средства коммуникации, установления связи с жертвой (WhatsApp, Skype, Viber, телефонные звонки и сообщения);

- приложения для вывода денежных средств (банк, интернет-магазины, биржа, игры, онлайн-кошелёк и другие);

- приложения, способствующие установлению удалённого доступа к мобильным устройствам (AnyDesk, AirDroid).

Самое сложное при совершении подобного рода преступных действий – это установление доверительных отношений с жертвой. Для этого мошенники чаще всего выступают в роле:

- службы безопасности;

- работниками банка;

- сотрудниками пенсионного фонда;

- представителями власти;

- родственниками, которые попали в трудную ситуацию.

Чаще всего сталкиваются с мошенниками, которые представляются сотрудниками банка. Они различными способами стремятся узнать личные данные и воспользоваться ими с целью перевода денежных средств. Как только им удаётся это сделать, действия начинают происходить уже в Web-версии банка пользователя [4, с. 947].

Каждый банк имеет свои методы противодействия таким мошенникам. Они делятся на:

- внутренние

- внешние.

Первый тип подразумевает внутреннюю безопасность банка, реализуемую в одностороннем порядке. К примеру, когда клиент совершает перевод, банк может его отклонить (заблокировать) в целях безопасности. Таким образом, клиенту для завершения операции требуется обратиться в банк или на горячую линию с целью подтверждения перевода. Также, при подозрении на мошеннические действия в личном кабинете клиента, служба безопасности может также заблокировать учётную запись. Тогда клиенту надо прийти в отделении банка и подтвердить последние операции путём разблокировки

личного кабинета. В некоторых случаях разблокировку можно совершить самостоятельно через банкомат [5, с. 829].

Второй тип содержит способы, совершаемые уже непосредственно по инициативе клиента:

- блокировка личного кабинета путём обращения на горячую линию;
- подключение страховых услуг.

Способы, предоставляемые клиенту банком с целью сохранения денежных средств, у каждой кредитной организации различны, а также и условия их обеспечения. Например, в банке «ВТБ» (ПАО) предусмотрены такие платные услуги, как страхование от мошенничества (защита счёта клиента) и страхование кредитных карт. Они подразумевают то, что, при хищении денежных средств с застрахованных счетов, банк возмещает сумму денежных средств в рамках страхового случая и подключённой услуги. Для лиц, получающих пенсионные выплаты на счета банка «ВТБ» (ПАО), предусмотрено бесплатное страхование счета от мошеннических действий на сумму до 100 000 рублей. Данные продукты были введены и активно используются в результате увеличения случаев преступных действий путём вывода денежных средств с банковских счетов пользователей [1].

Мошеннические действия с использованием мобильных устройств можно разделить на два типа. В первом варианте, потерпевший самостоятельно сообщает свои конфиденциальные данные в результате манипуляций. Во втором случае, клиент скачивает на мобильное устройство приложение, позволяющее установить удалённый доступ мошенникам. Таким образом, человек теряет контроль над устройством, а пароли и данные, вводимые на экране и находящиеся в памяти телефона (планшета), отображаются у преступников.

В результате клиенты, по отношению к которым были совершены мошеннические действия, в первую очередь обращаются в банк, с которого были выведены денежные средства. Но банк не способен предотвратить действия и возместить ущерб, если клиент самостоятельно сообщает свои данные

мошенникам. Поэтому и были разработаны услуги коллективного страхования счетов, как было выше упомянуто на примере банка «ВТБ» (ПАО) [3, с. 34].

Основная информация, которая поможет клиентам банков не оказаться жертвой «телефонных мошенников»: во-первых, сотрудник банка может позвонить клиенту либо с целью рекламы нового продукта или же информировании о проходящей акции, либо с просьбой оценить качество обслуживания, но никто не будет требовать оформить кредитный продукт через телефон. Также, служба безопасности при подозрении на мошеннические действия не звонит клиенту, а блокирует учётную запись, чтобы предотвратить хищение денежных средств. Индивидуальные клиентские данные невозможно изменить по телефону, а только в отделении банка при личном обращении или, в редких случаях и не в каждом банке, через банкомат, например, номер телефона (клиент ПАО «Сбербанк»).

Чаще всего жертвами таких преступлений становятся лица пожилого возраста, женщины и девушки в возрасте 20-35 лет. Мошенники манипулируют ими, используя ложную информацию о состоянии их близких, сбережений и личных данных. В результате опроса, проведённого среду посетителей банка, каждый 3 человек обращается за консультацией и помощью по поводу мошенничества. Из 100 человек опрошенных, 93 сталкивались либо сами, либо их знакомые с мошенническими действиями, а 10% из них стали жертвами. Опрошенное население пенсионного возраста предпочтительнее считают тот банк, который способен гарантировать сохранность денежных средств и предоставляет страховые льготы [2, с. 115].

Более половины опрошенных клиентов установили приложения и дополнительные функции для распознавания входящих звонков. Но, тем не менее, население по-прежнему не осведомленно о существовании официальных горячих линий служб и организаций, которыми они пользуются. Например, только 69% опрошенных указали, что номер «1000» является горячей линией Банка ВТБ (ПАО).

Сообщая свои данные третьим лицам, клиент самостоятельно предоставляет доступы к своим денежным средствам. В таких случаях никакое улучшение системы безопасности и контроля не сможет предотвратить хищение. Только осторожность и внимательность к звонкам и сообщениям от посторонних может помочь сохранить сбережения.

Библиографический список:

1. Банк ВТБ (ПАО): Страхование от мошенничества - официальный сайт - URL: https://www.vtb.ru/personal/drugie-uslugi/strahovye-i-servisnye-produkty/zashhita-ot-moshennikov/ (дата обращения: 22.11.2023).

2. Внуков, А. А. Защита информации в банковских системах: учебное пособие для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2023. — 246 с. — (Высшее образование). — ISBN 978-5-534-01679-6. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512269 (дата обращения: 01.12.2023).

3. Гобозов, М. Д. Конфиденциальная защита банка / М. Д. Гобозов, Е. Н. Акоева, С. В. Акоева // ИННОВАЦИОННЫЕ ИДЕИ МОЛОДЫХ ИССЛЕДОВАТЕЛЕЙ: сборник статей Международного научно-исследовательского конкурса, Пенза, 20 июня 2021 года. – Пенза: Общество с ограниченной ответственностью "Наука и Просвещение", 2021. – С. 34-36. – EDN NFIIRI.

4. Фаллер, Г. В. Факторы риска и правовое обеспечение безопасности банковской деятельности в сфере дистанционного обслуживания / Г. В. Фаллер // Право и правосудие в современном мире : Сборник научных статей молодых исследователей XI Всероссийской студенческой научно-практической конференции студентов, магистрантов и соискателей (к 25-летию Российского государственного университета правосудия и 20-летию Северо-Западного филиала Российского государственного университета правосудия), Санкт-

Петербург, 24–25 марта 2023 года. – Санкт-Петербург: Центр научно-информационных технологий "Астерион", 2023. – С. 945-950. – EDN TZJDBT.

5. Явинский, А. В. Способы борьбы с телефонными мошенниками / А. В. Явинский, А. А. Соловьев // Образование. Транспорт. Инновации. Строительство: Сборник материалов IV Национальной научно-практической конференции, Омск, 22–23 апреля 2021 года. – Омск: Сибирский государственный автомобильно-дорожный университет (СибАДИ), 2021. – С. 828-831. – EDN IIECJE.

Оригинальность 99%