Вестник Сибирского юридического института МВД России

УДК 343.71 DOI 10.51980/2542-1735_2021_2_64

Сергей Юрьевич ДЕМЕНЕВ,
заместитель начальника отдела – начальник отделения компьютерных экспертиз 6-го отдела ЭКЦ ГУ МВД России по Красноярскому краю
demenevssb@mail.ru

Николай Владиславович ПОЛЯКОВ,
преподаватель кафедры криминалистики Сибирского юридического института МВД России (г. Красноярск)
polyakov.nikolay.1987@mail.ru

ХИЩЕНИЕ ДЕНЕЖНЫХ СРЕДСТВ С РАСЧЕТНЫХ СЧЕТОВ ГРАЖДАН С ИСПОЛЬЗОВАНИЕМ УДАЛЕННОГО ДОСТУПА К МОБИЛЬНОМУ ТЕЛЕФОНУ

THEFT OF FUNDS FROM CITIZENS' SETTLEMENT ACCOUNTS USING REMOTE ACCESS TO A MOBILE PHONE

Статья посвящена рассмотрению типичных способов совершения хищений денежных средств со счетов граждан путем использования программ удаленного доступа к телефону. Анализ судебно-следственной практики по рассматриваемой категории уголовных дел показывает, что их расследование вызывает у следователей трудности как в сборе доказательственной информации, так и в доказывании виновности причастных к ней лиц. В связи с этим в работе обращается внимание на ряд проблемных вопросов, возникающих в процессе расследования.

The article is devoted to the examination of typical ways of committing thefts of funds from citizens' accounts by using remote phone access programs. The analysis of the judicial and investigative practice on the considered category of criminal cases shows that their investigation causes the investigators difficulties, both in collecting evidentiary information and in proving the guilt of the persons involved. In this regard, the authors draw attention to a number of problematic issues arising in the course of the investigation.

Ключевые слова: системы дистанционного банковского обслуживания, кража, мошенничество, денежные средства, расчетный счет, правовое просвещение.

Keywords: *remote banking systems, theft, fraud, monetary funds, settlement account, legal education.*

Глобальный курс российского государства на цифровизацию экономики, повсеместное распространение Интернета, а также переход от расчетов наличными денежными средствами к электронным платежам способствуют быстрому развитию систем дистанционного банковского обслуживания.

В современном мире сложно найти человека, у которого нет мобильного телефона, большинство из которых смартфоны. Смартфон – сложное устройство, по сути, это носимый компьютер с функциями голосовой связи, обладающий значительной вычислительной мощностью и функционалом.

Кроме того, в последние годы получили широкое распространение программы удаленного доступа к компьютерным и мобильным устройствам, которые позволяют

осуществлять техническую поддержку пользователей (владельцев) без выезда и физического присутствия возле них. Такие программы существуют для операционных систем Android и iOS.

В 2019 г. Российская Федерация находилась на первом месте в мире по количеству клиентов, которые пользуются мобильными банковскими приложениями. Согласно статистическим данным, доля активных клиентов банков, воспользовавшихся мобильным приложением в России хотя бы раз за 90 дней, в 2019 г. составляла 36,2%. Для сравнения: указанный показатель во всем мире составил 28,1%[1].

Согласно проведенным исследованиям, на свои устройства с операционной системой Android более 100 млн пользователей скачали мобильные приложения Сбербанка, ВТБ, Альфа-банка, банка Тинькофф – более 10 млн каждого. Как видно, доля Сбербанка кратно превосходит остальные банки и, соответственно, его клиенты чаще всего становятся жертвами различного рода мошенников.

Технология позволяет осуществлять практически любые действия с устройством, чем и пользуются преступники. Потерпевшими по уголовным делам, как правило, становятся люди старшего и пожилого возрастов, которым родственники купили смартфоны для приобщения к современным технологиям. Однако данная категория граждан не до конца осознает возможности, которыми обладает устройство, и какую опасность они могут представлять. При этом в ходе получения банковской карты вежливые сотрудники кредитных организаций предлагают клиентам подключить услугу мобильного банка, мотивируя это удобством, простотой использования и отсутствием потребности посещать отделение банка.

Хищение денежных средств с банковских карт путем обмана или злоупотребления доверием квалифицируется по ст.159.3 УК РФ. В 2019 г. в Российской Федерации зарегистрированы 10826 указанных преступлений. В первом полугодии 2020 г. количество мошенничеств с использованием электронных средств платежей возросло на 103,6%[2].

Одной из причин появления данного вида мошенничества стало совершенствование защиты мобильных устройств от вирусов. Кроме того, рассматриваемый способ мошенничества достаточно просто реализуем в техническом плане, но требует от злоумышленников развитого навыка убеждения, чтобы втереться в доверие к жертве и заставить ее совершать необходимые действия.

Преступники, владея информацией о наличии счетов клиентов в банках и их личными данными, при общении сообщают последним, что они стали жертвами мошенников, а они, выполняя свой долг и защищая от опасности, могут им помочь. Потерпевшим, как правило, поступает звонок, при этом на экране телефона может высвечиваться номер, начинающийся цифрами 8 800, либо номер, схожий со справочной службой банка, либо номер любого региона России. Современные виртуальные АТС позволяют это реализовать, все зависит от фантазии преступников.

Кроме того, ими может проводиться рассылка SMS, содержащих информацию о подозрительных переводах денежных средств и указание номера службы безопасности, по которому необходимо перезвонить. В этой ситуации взволнованные потерпевшие, идентифицируя преступников с сотрудником банка, сами звонят им, тем самым подтверждая свое желание решить несуществующую проблему и готовность выполнять любые указания. Злоумышленники представляются сотрудниками безопасности банка и, обладая необходимой информацией, обращаются к жертве по имени и отчеству, могут сообщить текущий баланс, тем самым в сознании граждан происходит аутентификация преступника как «своего». Затем задаются вопросы о том, совершала ли жертва перевод на определенную сумму вымышленному лицу. Жертва же, конечно, никому ничего не переводила и начинает переживать за сохранность своих

1 Газета Коммерсант. URL: https://www.kommersant.ru/doc/4102921 (дата обращения: 04.03.2021).
2 Министерство внутренних дел Российской Федерации. URL: https://мвд.рф/reports/item/23163626/ (дата обращения: 04.03.2021).

сбережений. Злоумышленник, понимая, что лицо «на крючке», сообщает, что для предотвращения хищения денежных средств нужно срочное вмешательство в работу банковского приложения, для чего надо установить «специальный антивирус» из PlayМаркета. На самом же деле данным приложением является программа удаленного доступа, но жертва все равно не разбирается в этом, все ее мысли и внимание заняты спасением накоплений.

После установки приложения лицо просят сообщить идентификатор и в зависимости от используемой программы либо пароль для доступа, либо подтверждение запроса на подключение. Затем требуют открыть приложение мобильного банка, ввести пароль, чтобы получить к нему доступ, отложить смартфон и не трогать его, чтобы не мешать работе «антивируса». Также распространенным предлогом для вмешательства в смартфон жертвы являются технические неполадки в банковской системе, которые могут привести к потере накоплений, для сохранения которых необходимо перевести деньги на «специальный счет» банка-партнера.

Таким образом, в ход идут методы социальной инженерии, которые подразумевают использование доверия жертвы, которую убеждают установить на телефон какое-либо приложение для осуществления удаленного доступа. В качестве аргументации преступники используют различные поводы. При этом лицо, находясь в стрессовой ситуации, следует инструкциям, не задумываясь о сути производимых операций.

Получив полный доступ к устройству, преступники переводят денежные средства на подконтрольные им банковские карты, оформленные, как правило, на подставных лиц, по номеру телефона и подтверждают операции по списанию денежных средств кодами из SMS.

В настоящее время в связи с созданием единой системы быстрых платежей информацию о том, есть ли у гражданина счет в банке, получить достаточно просто. Для этого нужно в мобильном банковском приложении указать номер телефона и приложение отобразит счета, в каких банках есть у предполагаемой жертвы, а также ее имя и отчество.

При проведении комплекса мероприятий по установлению преступников возникают сложности, связанные с тем, что произошедшее для кредитной организации выглядит как законные действия владельца, так как переводы осуществляются с его устройства, на которое приходят сообщения с кодами подтверждения (двухфакторная аутентификация), при этом на смартфоне отсутствует вредоносное программное обеспечение. Удаленные подключения хоть и фиксируются в памяти смартфона жертвы, но сами действия по переводу денежных средств, выполняемые преступниками, не фиксируются. Кроме того, потерпевшие, осознав произошедшее, в панике сами удаляют приложение для удаленного доступа или вовсе сбрасывают телефон к заводским настройкам с автоматическим стиранием памяти.

Стоит отметить, что существованию данного вида мошенничества способствует недостаток знаний у клиентов банков о функционировании как смартфонов, так и системы дистанционного банковского обслуживания в целом. В рекламе, средствах массовой информации и от сотрудников банков обычно исходит информация о преимуществах сервиса, а на возможные отрицательные последствия и уязвимости сервиса акцент не делается, чтобы не пугать клиента. Также важнейшим фактором, способствующим распространению мошенничества, является доверчивость граждан, особенно старшего и пожилого возрастов, которые привыкли доверять людям, представляющимся от имени организаций с названиями «служба» или «безопасность». Имеются и недостатки в работе мобильных банков. Так, современные приложения могут определять, происходило ли потенциально опасное вмешательство в защиту операционной системы телефона (получение root-доступа), и зачастую имеют встроенный антивирус, но не реагируют на наличие запущенных программ для обеспечения удаленного доступа к смартфону.

Наиболее действенным методом профилактики является правовое просвещение граждан о данном способе мошенничества, особенно через средства массовой информации, которым привыкли доверять люди старшего и пожилого возрастов, которые чаще других становятся жертвами злоумышленников. Также необходимо совершенствовать защиту мобильных приложений банков так, чтобы только владелец смартфона мог осуществлять платежи, исключая возможности воздействия на данный процесс третьих лиц.

Несомненно, что мероприятия, проводимые в рамках антикриминального просвещения, существенно повысят уровень правовой культуры и грамотности населения [подр.: 1, с. 47].

Библиографический список

1. Поляков, Н.В. Антикриминальное просвещение индивидуальных предпринимателей и юридических лиц в рамках расследования уголовных дел как средство профилактики незаконных обналичивания и транзитирования денежных средств / Н.В. Поляков, С.А. Линник // Научный компонент. – 2019. – N 2 (2). – С. 43-47.