БЖАХОВ Гумар Мухамедович,
преподаватель кафедры
специальных дисциплин,
майор полиции
Северо-Кавказский институт
повышения квалификации (филиал)
Краснодарского университета
МВД России,
г. Нальчик, Россия,
e-mail: mail@law-books.ru

РАСПРОСТРАНЕННЫЕ СХЕМЫ, КОТОРЫМИ ПОЛЬЗУЮТСЯ МОШЕННИКИ В 2024 ГОДУ, ЧТОБЫ ЗАВЛАДЕТЬ ЧУЖИМ ИМУЩЕСТВОМ

АННОТАЦИЯ. Целью данного исследования Преступления совершенные под предлогом оказания социальных услуг приходится 90 процентов всех финансовых преступлений, причем 94 процента из них — это телефонное мошенничество.

Задачи исследования состоят в проведении анализа совершения телефонное мошенничества, которая является основным способом выманивания денег у граждан России. По мере совершенствования системы кибербезопасности растут и возможности аферистов, которые придумывают все новые способы завладения чужим имуществом при помощи телефона и интернета.

Выводы: автор обращает внимание на признаки и последствия дистанционного мошенничества, которые становится все более серьезной проблемой: в 2024 году с попытками обмана по телефону или интернету столкнулись 85 процента жителей нашей страны. В связи с чем, необходимо проводить профилактические и воспитательные мероприятия.

КЛЮЧЕВЫЕ СЛОВА: дистанционное мошенничество, кибербезопасность, кибермошенничество, фишинг, телефонное мошенничество.

BZHAKHOV Gumar Mukhamedovich,
lecturer of the Department of Special Disciplines,
Police Major North Caucasus Institute of Advanced
Training (branch) of Krasnodar University
of the Ministry of Internal Affairs of Russia,
Nalchik, Russia

COMMON SCHEMES USED BY SCAMMERS IN 2024 TO TAKE POSSESSION OF OTHER PEOPLE'S PROPERTY

ANNOTATION. The purpose of this study is crimes committed under the pretext of providing social services account for 90 percent of all financial crimes, and 94 percent of them are telephone fraud.

The objectives of the study are to analyze the commission of telephone fraud, which is the main way to extort money from Russian citizens. As the cybersecurity system improves, the possibilities of scammers are also growing, who come up with new ways to seize other people's property using the phone and the Internet.

Conclusions: the author draws attention to the signs and consequences of remote fraud, which is becoming an increasingly serious problem: in 2024, 85 percent of the inhabitants of our country faced attempts to cheat by phone or the Internet. In this regard, it is necessary to carry out preventive and educational measures.

KEY WORDS: remote fraud, cybersecurity, cyber fraud, phishing, telephone fraud.

Дистанционное мошенничество становится все более серьезной проблемой: в 2024 году с попытками обмана по телефону или интернету столкнулись 85 процента жителей нашей страны. По данным специалистов в области кибербезопасности, объем совершенных

мошенничеств в 2024 году в России на сегодня оценивается в сумму от 55 до 150 миллиардов рублей.

Преступления совершенные под предлогом оказания социальных услуг приходится 90 процентов всех финансовых преступлений, причем 94 процента из них — это телефонное мошенничество. По мере совершенствования системы кибербезопасности растут и возможности аферистов, которые придумывают все новые способы завладения чужим имуществом при помощи телефона и интернета. 24 июля 2023 года был принят закон, который должен усложнить их жизнь: банки смогут замораживать деньги после подозрительных операций.

Сколько денег теряют россияне по вине мошенников

Телефонное мошенничество является основным способом выманивания денег у граждан России: в 2023 году на этот вид незаконной деятельности пришлось около 92 процентов основных схем, применяемых киберпреступниками. По вине телефонных мошенников в прошлом году в России было похищено около 14 миллиардов рублей преступным путем мошенниками. Причем не исключено, что в действительности дистанционным путем было похищено еще больше денег. К столь неутешительным выводам эксперты приходят на основе зарегистрированных преступлений в правоохранительных органах [1].

С попыткой кибермошенничества на территорий России сталкиваются около 83 процентов людей. В общей сложности было зафиксировано около пяти миллиардов попыток мобильного мошенничества. В своих схемах аферисты прибегают к использованию роботизированных виртуальных ассистентов. Чаще всего звонки с подменных номеров поступают россиянам из-за границы: в лидеры по этому показателю выбились Украина, Польша, Казахстан, Таджикистан, Белоруссия. Через форму обратной связи в мобильном приложении банков около 1.8 миллионов клиентов обращаются по данной проблеме [3].

Снижать свою активность преступники явно не планируют и, напротив, лишь расширяют масштабы своей преступной деятельности. В настоящее время они используют для совершения преступления не только звонки с подменой номера, но и различные социальные сети и звонки с помощью DEF-номеров, когда телефонный код не привязан к географическому расположению [2].

Схемы мошенничества

Одна из старейших преступных мошеннических схем, применяемых до сих пор, направлена на пожилых людей: это трюк с «попавшим в беду родственником». Скорее всего, почти все о нем слышали: звонящий в крайне эмоциональном тоне убеждает, что близкий вам человек стал виновником ДТП, попался с наркотиками или совершил какое-либо другое серьезное преступление. Как следует запугав собеседника и добившись желаемого психологического эффекта, преступник затем заговорщицки намекает, что «можно решить вопрос» — и родственник избежит положенного наказания за совершенное преступление. Затем трубку передают «сотруднику правоохранительных органов», который развивает напор и уточняет детали.

В зависимости от наглости мошенников сумма может варьироваться от 20-30 тысяч рублей до миллиона и даже больше. Деньги потребуют либо перевести сразу на карту, либо передать посреднику (обычно их нанимают из числа курьеров или таксистов, которые после чего попадаются полицейским).

Звонок из «службы безопасности банка»

Одним из способов совершения преступления является звонок от «сотрудника службы безопасности банка»: преступник сходу огорошивает заявлением о том, что с карты клиента прямо сейчас пытаются списать крупную сумму, и чтобы этого не случилось, надо назвать звонящему номер карты, CVV-код и код из СМС. Так мошенники получают доступ к денежным средствам своих жертв. Этот прием уже хорошо известен, но люди продолжают попадать в ловушку. В большинстве случаев мошенники действуют чисто интуитивно, они не знают, ни в каких банках обслуживается клиент, ни сколько денег он имеет на счете.

Ошибочный перевод

Распространенным видом мошенничества является ошибочный перевод: человека убеждают в том, что на его мобильный телефон или на банковскую карту ошибочно перевели определенную сумму денежных средств. В подтверждение этих слов приходит сообщение о зачислении средств. Расчет идет на то, что жертва почувствует себя неловко и поспешит вернуть деньги. Подвох же в том, что «ошибочный» перевод был на ничтожную сумму (например, 20 рублей, что легко принять за 2000), либо его не было вовсе, а сообщение с замаскированного телефонного номера послали сами мошенники [4].

«Поздравляем, вы выиграли в лотерею»

Для прикрытия своих преступлений мошенники часто используют рекламные акции, лоте-

реи или розыгрыши. Звонящий может представиться ведущим. Вначале он поздравляет с крупным выигрышем в лотерею — это может быть телефон, ноутбук или автомобиль. Затем доверчивую жертву переключают на «сотрудника призового отдела», и тот уже разводит на личные данные.

Трюк с просьбой перезвонить от знакомого

Существует мошенническая схема с номером-грабителем, когда человеку приходит СМС с просьбой от знакомого человека перезвонить на незнакомый телефонный номер, что объясняется веской причиной: срочно требуется помощь, проблемы со связью и т. д. После звонка человека долго держат на линии, и за это время с лицевого счета списываются большие суммы [5].

Обман по СМС

Мошенничество совершенное с использованием СМС сообщений. Мошенник отправляет от лица финансовых организаций СМС сообщение. Как правило, абонентам приходят сообщения об одобренном кредите или займе (при этом сам человек ни в какие банки или МФО не обращался).

Такие СМС сообщения составляют по схожему шаблону: вверху — кричащая и при этом короткая фраза, способная если не заинтересовать, то точно привлечь внимание. Например, «сумма пересмотрена — получите 21500 руб.», «ув. клиент, вам одобрили заем на 13500 руб.» и т. д. Далее находится ссылка, по которой нужно пройти для завершения процедуры получения денег. На самом деле переход по такой ссылке не сулит ничего хорошего.

Цель преступников — заманить доверчивого и, видимо, испытывающего потребность в денежных средствах человека на вредоносный сайт и похитить его персональные данные, чтобы затем использовать их в других мошеннических схемах или продать другим мошенникам.

Фишинг

В интернет пространстве основной инструмент мошенников — фишинг. Злоумышленники создают поддельные сайты, заманивают на них жертв и похищают данные банковских карт. Причем мишенью жуликов становятся даже дети, для которых создают фейковые аналоги магазинов цифровой техники, а также магазинов онлайн-игр и аксессуаров для них. Их завлекают низкими ценами. Нередко киберпреступники используют образы популярных блогеров.

Подростков пытаются привлечь объявлениями о быстром и легком заработке, убеждают вложить деньги в «сверхвыгодный проект», имитируют инвестиционные онлайн-игры. Так ребенок рискует оказаться втянутым в махинации с нелегальным движением средств. Зафиксированы случаи, когда мошенники прикидывались ровесниками и выманивали у подростков данные родительских карт.

На вас пытаются взять кредит

Еще один популярный метод похищения денежных средств обманным путем — «звонок из Центробанка». Чаще звонить пытаются через различные социальные сети, чтобы вместо номера определялся аккаунт, на аватаре которого — российский герб и название организации (хотя с физическими лицами Центральный банк не работает вообще. Впрочем, иногда мошенники звонят с аккаунта, подписанного «МВД России»).

В ходе телефонного разговора мошенник говорит, что кто-то пытается получить на вас кредит, и, чтобы не платить по чужим долгам, эти кредитные деньги нужно срочно забрать в отделении банка или перевести на «безопасный счет».

Как защититься от мошенничества

Эксперты в области дистанционных мошеничеств констатируют, что преступники постоянно меняют тактику, придумывают новые способы совершения мошеннических действий на фоне возросших потребностей пользователей интернета в области безопасности. Но абсолютной защиты от них не существует. При разъяснении рисков и угроз населению сотрудники банков обычно напоминают, что сотрудники службы безопасности банков никогда не связываются с клиентами банка сами — общение с владельцами банковских карт попросту не входит в перечень их полномочий. Поэтому все вопросы, связанные с движением денежных средств и соблюдением норм безопасности, можно решать только при личном визите клиента с паспортом в отделение банка [6].

Сотрудники полиции регулярно проводят профилактические мероприятия направленные на своевременное предупреждение для предотвращения жителей обслуживаемой территории совершения в отношений них мошеннических действий преступниками.

Нельзя сообщать кому-либо свои персональные данные, особенно пароли от личного кабинета, номера и PIN-коды банковских карт. Категорически нежелательно хранить такую информацию на компьютере или в смартфоне, а

тем более на бумажке в кошельке. Нельзя переходить по сомнительным ссылкам, особенно присланным в СМС с подозрительного номера.

Обратите внимание: чтобы точно не нарваться на мошенников, следует игнорировать звонки с незнакомых телефонных номеров и сразу же пробивать их в любом из поисковиков в интернете. Информацию о номерах, которыми пользуются злоумышленники, собирают специальные сайты — там делятся опытом абоненты, которых пытались обмануть до вас. Если номер, с которого вам звонили, оценен отрицательно, смело заносите его в черный список. Если же вы ответили на звонок — поспешите закончить общение и ни в коем случае не следуйте указаниям по телефону от незнакомых лиц, даже если они представляются сотрудниками банка или полиции.

Кстати, Сбербанк собирает базу голосов киберпреступников, которые пытаются обмануть клиентов по телефону, и способен автоматически блокировать спровоцированную ими транзакцию.

Услуги по защите от мошенничества предоставляют различные организации, занимающиеся формированием, обработкой и хранением кредитных историй. Например, НБКИ предлагает платную годовую подписку, которая позволит «защитить себя от действий злоумышленников». Как уточняется на сайте бюро, как только в кредитной истории клиента появится новый кредит, заем или данные другого паспорта, ему придет уведомление по СМС.

И крайне важно ввести в своих аккаунтах в интернете двухфакторную аутентификацию, если она еще не работает. Доступа просто по паролю недостаточно, чтобы обезопасить свои данные.

Согласно словам эксперта по кибербезопасности ГУ Банка России по ЦФО Алексея Потехина, детей необходимо с ранних лет приучать к бдительности в интернете.

«Очень важно донести до ребенка мысль, что надо крайне аккуратно делиться в интернете личной информацией, — подчеркнул он. — Объясните ему, что не надо сообщать ничего лишнего о себе, своей семье и своей жизни в соцсетях, на форумах и на любых других онлайн-площадках».

Что делать, если вы уже стали жертвой мошенников

Если вы обнаружили факт мошенничества, то алгоритм действий прост.

1. Подайте заявление в полицию по ст.159 Уголовного кодекса.
2. Обратитесь к кредитору с претензией, укажите в ней на факт мошеннических действий и изложите обстоятельства дела.
3. Приложите к письму талон-уведомление из полиции, предоставьте справку об утрате удостоверения личности (при наличии), свидетельские показания, записи с камер в помещении, где был оформлен кредит и подтверждения вашего алиби.
4. Соберите справки о состоянии счетов и об истории операций в обслуживающих банках в качестве доказательства отсутствия переводов от МФО. Передайте заверенные копии кредитору.
5. Если речь идет об онлайн-займе, нужно указать кредитору на то, что он оформлен не на ваш мобильный номер.
6. Передайте следователю, который работает с вашим делом, все собранные документы по делу.
7. Попробуйте добиться решения ситуации мирным путем. Если не получается, обратитесь к юристу.

Часто кредиторы решают проблему в досудебном порядке в течение семи-десяти дней с момента обращения потерпевшего. Настоящие сотрудники службы безопасности проведут проверку, выяснят обстоятельства, аннулируют долг и удалят запись из БКИ. Банки и МФО легче отказываются от требования незначительных сумм, но если задолженность крупная, то могут и не пойти навстречу.

Статистика по раскрываемости киберпреступлений в каждом регионе разная. Например, в Алтайском крае по итогам 2022 года она составила чуть больше 30 процентов.

По мнению экспертов, раскрытию таких преступлений мешает потеря времени с момента совершения махинации, отсутствие тесного взаимодействия полиции с банками и мобильными операторами. К моменту заведения уголовного дела преступники уже выводят все деньги со счетов.

Список литературы:

[1] Вне зоны доступа. Зэки массово выманивают у россиян деньги. Тюрьмы их защищают: Следствие и суд: Силовые структуры: Lenta.ru /URL: https://lenta.ru/articles/2018/05/24/extortion/ (дата обращения 29.04.2022)

[2] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) \ КонсультантПлюс

[3] Кудрявцев Р.В. Организация деятельности по раскрытию дистанционных мошенничеств// Молодой ученый. - 2019. - № 24 (262). - С. 218-221.

[4] Мошенничество в сети: судебная практика и главное - RTM Group / URL: https://rtmtech.ru/research/online-fraud-research/ (дата обращения 29.04.2022)

[5] Машекуашева М.Х. О значимости информационно-психологической защиты индивида и социума: особенности воздействующего потенциала. Право и управление. 2024. № 2. С. 375-377.

[6] Уголовный кодекс Российской Федерации (УК РФ) от 13.06.1996 № 63-ФЗ (последняя редакция) \ КонсультантПлюс.

Spisok literatury:

[1] Vne zony dostupa. Zeki massovo vymanivayut u rossiyan den'gi. Tyur'my ih zashchishchayut: Sledstvie i sud: Silovye struktury: Lenta.ru /URL: https://lenta.ru/articles/2018/05/24/extortion/ (data obrashcheniya 29.04.2022)

[2] Konstituciya Rossijskoj Federacii (prinyata vsenarodnym golosovaniem 12.12.1993 s izmeneniyami, odobrennymi v hode obshcherossijskogo golosovaniya 01.07.2020) \ Konsul'tantPlyus

[3] Kudryavcev R.V. Organizaciya deyatel'nosti po raskrytiyu distancionnyh moshennichestv// Molodoj uchenyj. - 2019. - № 24 (262). - S. 218-221.

[4] Moshennichestvo v seti: sudebnaya praktika i glavnoe - RTM Group / URL: https://rtmtech.ru/research/online-fraud-research/ (data obrashcheniya 29.04.2022)

[5] Mashekuasheva M.H. O znachimosti informacionno-psihologicheskoj zashchity individa i sociuma: osobennosti vozdejstvuyushchego potenciala. Pravo i upravlenie. 2024. № 2. S. 375-377.

[6] Ugolovnyj kodeks Rossijskoj Federacii (UK RF) ot 13.06.1996 № 63-FZ (poslednyaya redakciya) \ Konsul'tantPlyus.