На сегодняшний день в Кировской области остается сложной ситуация с дистанционными хищениями.

За 8 месяцев 2024 года в органах внутренних дел на территории Кировской области зарегистрировано 3780 преступлений, которые были совершены в отношении жителей региона с использованием информационно-телекоммуникационных технологий. В их числе квалифицированные по статьям 158 (кража), 159 (мошенничество), 163 (вымогательство) Уголовного кодекса Российской Федерации. По сравнению с прошлым годом прирост составил 12,8%. Суммарный ущерб, причиненный потерпевшим, превысил 955 миллионов рублей.

Наиболее распространенные способы совершения дистанционных хищений:

Звонок «сотрудника банка» или «сотрудника правоохранительных органов».

В разговорах с потенциальной жертвой по телефону или в мессенджерах «Ватсап», «Вайбер», «Телеграм» мошенники представляются сотрудниками коммерческих банков, Центрального банка России, работниками безопасности или службы финансового мониторинга. С их слов, кто-то якобы пытается оформить кредит от лица потерпевшего, а также обналичить и похитить сбережения. Нередко сообщается о якобы имеющих место попытках преступников «по похищенным персональным данным» завладеть имуществом (автомобилями, недвижимостью).

Под этим предлогом мошенники предлагают гражданину обезопасить себя от несанкционированного оформления кредита, хищения сбережений и имущества. Следуя указаниям, потерпевший получает заем, своей заявкой якобы отменяя заявку мошенника. Обналичив эти деньги вместе со своими сбережениями, он переводит по диктуемым номерам чьих-то карт, счетов, телефонов, обозначенные как «безопасный/специальный/защищенный счет». Нередко злоумышленники называют реквизиты «защищенной банковской карты» для добавления в приложение бесконтактной оплаты на смартфоне. При ее пополнении потерпевший думает, что деньги остаются у него, но на самом деле доступа к средствам он больше не имеет.

Чтобы предотвратить хищения материального имущества, преступники так же предлагают совершить «фиктивные сделки»: продать квартиру/машину подставному лицу, а полученные деньги перевести на спецсчет.

При совершении хищений по этой схеме мошенники могут

представляться сотрудниками правоохранительных органов (МВД, ФСБ, прокуратура, Следственный комитет). Номер, с которого поступает звонок, на экране телефона может отражаться как настоящий номер организации, а при общении в мессенджере в профиле стоит фотография с символикой ведомства. Преступники просят сверить номера их телефонов с опубликованными на сайтах, могут пересылать фотографии служебных удостоверений. Все это делается для того, чтобы потерпевший полностью доверился и следовал их указаниям.

Характерные признаки манипуляции – звонящие ведут с потерпевшими длительное общение по телефону и полностью контролируют их действия. Инструктируют при общении с настоящими сотрудниками банка при оформлении кредита называть надуманные цели, а (на строительство, на лечение, срочная покупка).

При общении с потерпевшими преступники убеждают, что жертва «за чужие кредиты» может оказаться в долговой кабале на долгие годы. Они оказывают психологическое воздействие путем уговоров, угроз, повышенного тона, перекладывания вины на самого потерпевшего за отказ его следовать указаниям звонящего и потере денежных средств. При этом могут ссылаться при разговоре на статьи Уголовного кодекса Российской Федерации о неразглашении информации, за несоблюдение тайны следствия, за отказ от сотрудничества с правоохранительными органами, могут пугать большими штрафами.

В последнее время преступники, действующие под видом сотрудников силовых структур, запугивают граждан уголовной ответственностью за «финансирование запрещенных организаций, террористов, вооруженных сил зарубежных стран» и т.п. Якобы деньги со счетов потенциальной жертвы переводятся мошенниками на заграничные счета; возможность предотвратить это и не стать фигурантом уголовного дела – строгое следование инструкциям.

Еще один способ заставить потерпевшего поверить в необходимость выполнения инструкций – обратиться под видом знакомого человека. Чаще всего мошенник создает в мессенджере профиль с именем и фотографией руководителя потенциальной жертвы. От его лица он пишет потерпевшему о якобы идущих проверках работников на предмет неконтролируемых денежных переводов: предупреждает, что на связь выйдут сотрудники правоохранительных органов и нужно делать все, что они скажут.

Обратившейся в июле в полицию 43-летней кировчанке в мессенджере написал ее «директор»: якобы организацию и работников проверяют сотрудники ФСБ, нужно выполнять все их требования. Вышедшие следом на

связь незнакомцы, действительно, представились сотрудниками этой службы, а также Росфинмониторинга. По их словам, от лица женщины кто-то оформляет кредиты и похищает деньги. Для отмены чужих заявок ей самой нужно получить займы и отправить полученные средства на безопасный счет.

Жительница выполнила инструкции и только после этого поняла, что ее обманули, и обратилась в полицию. Ущерб составил 971 тысячу рублей, по факту мошенничества в крупном размере возбуждено уголовное дело.

Мошенники могут представляться также сотрудниками сервиса «Госуслуги», работниками оператора сотовой связи. Так в описанной выше схеме появляется еще один шаг: под предлогом продления действия сим-карты или договора обслуживания с мобильным оператором злоумышленники требуют назвать коды подтверждения из смс-сообщений от «Госуслуг». На самом деле с их помощью злоумышленники получают доступ к учетной записи жертвы и меняют пароль. В дальнейшем этот факт используется в качестве аргумента необходимости навязываемых мошенниками инструкций потерпевшему.

Стоит отметить, что мошенники могут продолжать откровенно издеваться над гражданами уже после совершения хищений денег. Зафиксированы случаи, когда потерпевшим в мессенджере приходили «благодарственные письма», «грамоты» с «официальным» подтверждением о переводе денег преступникам.

Иногда звонящие пользуются отчаянием жертвы, обещая вернуть похищенные деньги. Но для этого нужно выполнить какие-либо действия: записать видео с собственной клятвой верности запрещенной организации или совершить противоправное деяние, обычно связанное с порчей чужого имущества. В подразделениях полиции в регионах зафиксированы факты, когда граждан, к примеру, вынуждали прийти в банк и облить работников зеленкой или попытаться поджечь объекты государственного имущества. Что характерно, деньги даже в случае «успеха» жертвам так никто и не вернул. Вдобавок, их действия в ряде случаев были квалифицированы не только как административные правонарушения, но и преступления. Некоторые уже привлечены к ответственности.

Необходимо запомнить!

– Нельзя оформлять кредиты и переводить деньги по требованиям, полученным в ходе общения по телефону или в мессенджерах, кем бы ни представлялись собеседники! В банках не существует услуги «безопасных/защищенных/специальных счетов», куда нужно переводить

деньги для защиты от хищений.

– Нельзя называть телефонным собеседникам коды подтверждения операций из смс- или пуш-сообщений!

– Проверяйте всю информацию у компетентных лиц. Если есть основания переживать за сохранность денег на счетах, обратитесь в свой банк по телефонному номеру службы поддержки клиентов или лично в ближайшее отделение.

– Сотрудники правоохранительных органов не используют мессенджеры для связи с гражданами, не высылают фотографии своих служебных удостоверений и, тем более, не требуют от граждан оформлять кредиты и переводить куда-либо деньги.

– Сотрудники Центрального банка России в рамках своих полномочий не взаимодействуют с гражданами.

– Не переходите по присланным незнакомцами ссылкам на Интернет-страницы. Не устанавливайте на свои устройства приложения, программы по инструкциям, полученным по телефону или в мессенджере.

– При проявлении настойчивости звонящих, помните: это они первые вышли на связь с вами. Выполнение навязываемых инструкций нужно им, а не вам. Не теряйте голову. Руководствуйтесь в действиях здравым смыслом, а не эмоциями.

«Дополнительный заработок, биржа, инвестиции»

Потерпевший находит в сети Интернет предложение дополнительного пассивного дохода (инвестиции, биржевая торговля, криптовалюта и т.п.) и оставляет свои контакты. На связь с ним – по телефону или в мессенджерах – выходят лица под видом трейдеров, брокеров, финансовых консультантов. Они предлагают свою помощь: от лица потенциальной жертвы они будут выполнять все действия с финансовыми активами за процент.

Получив согласие, «помощники» предлагают зарегистрироваться на сайте биржи, создать онлайн-кошелек с криптовалютой или акциями .При этом деньги на финансовые операции нужно отправлять обычным банковским переводом по номеру карты или телефона. Такие «пополнения счета», а также прибыль от вложений жертва видит в своей учетной записи. Небольшую сумму дохода жертве действительно могут разово выплатить. Но это лишь уловка, чтобы потерпевший поверил в эффективность схемы заработка.

Злоумышленники убеждают в необходимости более крупной игры: чем больше вложишь, тем больше заработаешь. Нередко жертвы отправляют сотни тысяч и миллионы рублей, а «помощники» докладывают о кратном увеличении этих сумм. Однако в ответ на просьбу потерпевшего выдать доход со счета, под различными предлогами «брокеры» потребуют деньги на оплату налогов, страховок, комиссий, инкассацию, конвертацию валюты и т.д. В итоге вывода средств не произойдет, связь с «брокерами» прекратится, денежные средства останутся у них.

В полицию обратился житель Слободского района, 1979 года рождения: его обманул «представитель инвестиционной компании». Как выяснилось, ранее потерпевший согласился «получать дополнительный заработок». Интернет-собеседник пообещал помогать ему в «инвестициях в криптовалюту и драгоценные металлы». В результате потерпевший набрал в нескольких банках займы и перевел деньги на указанные ему счета, но обратно ничего не получил. Причиненный ущерб составил 7 миллионов рублей. Возбуждено уголовное дело по признакам преступления, предусмотренного частью 4 статьи 159 УК РФ.

Полиция призывает не верить предложениям большого и быстрого дохода в Сети. Самостоятельный заработок на инвестициях, биржевой торговле, криптовалюте требует специальных знаний. Стоит отметить, что большинство предложений заработка от мошенников в Сети реализуются по схеме «сначала заплати – потом получишь доход». Такое доверие малознакомымИнтернет-собеседникам без гарантий чревато потерей денег.

«Родственник в беде»

Этот вид обмана используется чаще в отношении пожилых граждан. На домашний телефон поступает звонок, в разговоре сообщается о попавшем в беду близком человеке. При этом либо потенциальная жертва сама «узнает» в собеседнике родственника, либо о происшествии сообщает «сотрудник полиции», «врач», «адвокат потерпевшего».

Как правило, речь идет о дорожно-транспортном происшествии, произошедшем по вине родственника. Решить проблему помогут деньги – будь то на оплату срочной операции пострадавшему или за «отказ от уголовного преследования». Обозначенную в разговоре сумму нужно передать специальному человеку («курьеру», «водителю»), который приедет домой к пожилому человеку.

Руководствуясь эмоциями, потерпевший выполняет телефонные

требования. К тому моменту, как он узнает, что с близким человеком на самом деле все было в порядке, курьер успеет перевести деньги на подконтрольные счета мошенников.

Пожилой кировчанке на стационарный телефон позвонил незнакомец, сообщивший о находящейся в больнице дочери женщины. Семья якобы попала в ДТП, виновником стал зять пенсионерки. Медицинская помощь пострадавшим в аварии не может быть оказана, пока не будет оплачена. Испугавшись, потерпевшая поверила. Пришедшему к ней домой незнакомцу она отдала 500 тысяч рублей.

Спустя час ей позвонили снова: переданных денег оказалось мало, нужно еще столько же. Пенсионерка согласилась и передала вновь пришедшему тому же молодому человеку еще один пакет с такой же суммой. Позже на связь спожилойкировчанкой вышла дочь: оказалось, у нее все в порядке, в ДТП она не попадала. В настоящий момент полицейские устанавливают личности причастных к совершению мошенничества.

Необходимо помнить:

– Нельзя отдавать деньги незнакомцам!

– Информацию о попавшем в беду родственнике нужно проверить, связавшись с ним или другими членами семьи по известным номерам телефонов.

– Настоящие сотрудники правоохранительных органов никогда не потребуют с вас денежные средства для урегулирования вопросов, так поступают только мошенники!

– Необходимо проинструктировать своих пожилых родственников, систематически напоминать им о таком способе обмана.