Обзор
о дистанционных кражах и мошенничествах в Ханты-Мансийском автономном округе – Югре, потерпевшими в результате совершения которых стали государственные и муниципальные служащие, сотрудники и работники бюджетной сферы, а также выявленных новых схемах мошенничеств, по итогам 4 квартала 2021 года

По информации Управления Министерства внутренних дел Российской Федерации по Ханты-Мансийскому автономному округу – Югре (далее – автономный округ) в четвертом квартале 2021 года органами внутренних дел автономного округа зарегистрировано 92 сообщения о преступлениях, предусмотренных ст.ст.158, 159 УК РФ, связанных с дистанционным хищением (завладением) денежных средств с банковских карт граждан, совершённых в отношении государственных и муниципальных служащих, сотрудников и работников бюджетной сферы.

В результате указанных противоправных действий пострадали представители исполнительных органов государственной власти автономного округа и их структурных подразделений, исполнительно-распорядительных органов городских округов и муниципальных районов автономного округа, педагогический состав и работники образовательных организаций автономного округа, медицинский персонал различного уровня системы здравоохранения.

Наиболее часто используемые мошенниками схемы, в ходе реализации которых произошло хищение денежных средств, следующие.

Звонки от сотрудников «службы безопасности банка» и сотрудников силовых структур (МВД, ФСБ, прокуратуры) с использованием SIP-телефонии и программ подмены абонентского номера, когда на телефоне потерпевшего определяется официальный номер банка, либо территориального органа МВД России, ФСБ и прокуратуры. При этом под предлогом пресечения сомнительных операций по счетам, оформления кредитов неизвестным лицом, либо под предлогом оказания помощи в установлении и поиске преступников среди сотрудников банков, предлагают оформить «зеркальный» кредит, а затем внести денежные средства на «безопасные ячейки», либо на абонентские номера, подконтрольные неизвестным лицам; сообщить номер банковской карты, CVC-код, а затем код в СМС сообщении, необходимый для удаленного управления и хищения денежных средств со счетов граждан.

В ходе продажи либо покупки товаров на сайтах бесплатных объявлений «Авито», «Юла», а также в социальных сетях «В контакте», «Одноклассники», «Инстаграмм» мошенники убеждают пройти по «безопасной ссылке», после чего денежные средства перечисляются на подконтрольные счета злоумышленников.

Оплата поездки с использованием сервиса «БлаБлаКар» по предоставляемой злоумышленником ссылке на предоплату в чате сервиса

или в мессенджере.

Перечисление денежных средств неизвестным лицам под предлогом участия в инвестиционных проектах на незарегистрированных Центральным Банком России «инвестиционных площадках».

Таким образом, в абсолютном большинстве случаев потерпевшие сами предоставили злоумышленникам информацию, с помощью которой последние незаконно завладели денежными средствами, либо перевели денежные средства на указанные им счета.

В целях профилактики фактов мошенничества и дистанционного хищения денежных средств следует принять во внимание следующую информацию.

Сотрудники служб безопасности банков не интересуются кодами, поступающими в СМС-сообщениях при совершении финансовых операций в «личном кабинете» клиента, не просят «клиентов» перевести денежные средства на резервные счета, не убеждают «клиентов» в необходимости оформления зеркальных кредитов с целью предотвращения «оформления кредита» на имя клиента неустановленными лицами, не интересуются наличием банковских карт сторонних банков и суммой денежных средств, находящихся на счетах клиента, не требуют перечисления денежных средств за «оформление, страхование, услуги курьера» при оформлении он-лайн кредитов.

Сотрудники правоохранительных органов при общении по телефону не сообщают о каких-либо мероприятиях, проводимых МВД, ФСБ и другими силовыми структурами, направленных на изобличение мошенников, не требуют от «клиентов банка» выполнять какие-либо инструкции сотрудников служб безопасности банков, не предупреждают об уголовной ответственности за невыполнение требований, поступающих в телефонном режиме от сотрудников банков.

При поступлении на телефон входящего звонка с абонентских номеров силовых структур (МВД, ФСБ, ФССП и т.п.), которые размещены на официальных сайтах, необходимо прекратить звонок и перезвонить на указанные номера самостоятельно. Важно дозвониться самому, а не ждать когда Вам перезвонят.

При поиске объявлений на сайтах «Юла», «Авито», «Дром», «Авто.ру» и других сайтах необходимо ознакомиться с правилами и условиями сайта, с правилами оплаты и предоплаты за покупку товара или за использование услуг доставки товара курьерской службой. Для осуществления безопасной сделки необходимо соблюдать ряд правил по их проведению, а именно:

«общаться» во внутреннем чате сайта и не уходить в другие мессенджеры;

хранить в тайне свою переписку, паспортные данные и код с карты;

не отправлять предоплату, если не уверены в порядочности продавца;

никому не сообщать коды из смс и push-уведомлений;

игнорировать ссылки на оплату, которые присылает собеседник.

При оформлении покупок на Интернет-сайтах, осуществлять мониторинг сети «Интернет» на предмет наличия отрицательных отзывов, а так же даты регистрации сайта. При условии, что сайт или страничка в соцсетях созданы недавно и отсутствуют отзывы, или имеющиеся отзывы носят отрицательный характер, то вероятнее всего они используются мошенниками. При совершении покупки необходимо обращать внимание на то, что у любого продавца имеется юридический адрес или адрес фактического нахождения магазина или склада. Информацию с указанием адресов магазинов можно проверить в сети интернет, например, на сервисах Яндекс или на сайте 2ГИС.

Осуществлять покупку билетов на различные виды транспорта необходимо исключительно с помощью официальных приложений, размещенных в «Appel Store» и «Play Market», а так же на официальных сайтах транспортных компаний, аэропортов и вокзалов. При этом важно помнить о нахождении в сети Интернет сайтов-двойников, которые могут иметь наименования, созвучные с официальными сайтами. Для исключения вероятности оформления покупки билетов на сайтах, созданных мошенниками, необходимо внимательно изучить весь сайт, перезвонить на телефон технической поддержки, уточнить у оператора всю информацию о предоставляемых услугах.