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 1 квартала 2022 года

По информации Управления Министерства внутренних дел Российской Федерации по Ханты-Мансийскому автономному округу – Югре (далее – автономный округ) в 1 квартале 2022 года отмечается снижение на 17,7% (с 1354 до 1114) количества зарегистрированных хищений, совершенных с использованием IT-технологий.

За 3 месяца текущего года органами внутренних дел автономного округа зарегистрировано 68 сообщений 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 происходит хищение денежных средств, и предложения по действиям, чтобы не стать жертвой мошенников:

1. 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, предлагается 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 случае поступления звонка с предложением выполнить вышеуказанные действия необходимо прекратить его, не выполняя никаких «рекомендаций». В сложившейся ситуации целесообразно самостоятельно перезвонить на номера, указанные на официальном сайте банка, территориального органа МВД России, ФСБ России, прокуратуры Российской Федерации, для уточнения причин звонка и получения информации.

2. В ходе продажи либо покупки товаров на сайтах бесплатных объявлений «Авито», «Юла», «Дром», «Авто.ру», а также в социальных сетях, оплаты поездки с использованием сервиса «БлаБлаКар», приобретения билетов на различные виды транспорта лица, использующие мошеннические схемы, убеждают пройти по «безопасной ссылке», после чего денежные средства перечисляются на подконтрольные счета злоумышленников.

В данном случае при поиске объявлений на 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.

Оформляя покупку на Интернет-сайтах, необходимо 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.