Обзор

о видах дистанционных краж и мошенничествах в Ханты-Мансийском автономном округе – Югре, а также выявленных новых схемах мошенничеств в 2021 году.

Данная тема остается актуальной, потому что потерпевшими от данного вида противоправных действий становятся не только простые граждане, но и 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 (*к примеру на территории Кондинского района за текущий период с указанных структур потерпевшими оказались 4 работника бюджетной сферы)*

Оперативная обстановка, связанная с применением при совершении правонарушений информационно – телекоммуникационных технологий остается сложной. Всего по информации Управления Министерства внутренних дел Российской Федерации по Ханты-Мансийскому автономному округу – Югре (далее – автономный округ) за период 2021 года на территории округа количество данных преступлений незначительно превысило показатель 2020 года на 0,4% (7618 фактов). с использованием информационных технологий. На территории Кондинского района зарегистрировано 35 таких преступлений что меньше по сравнению с аналогичным периодом прошлого года на 32%.

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

1. Завладение номерами банковских карт, кодами подтверждения операции из смс-сообщений от банка, cvc-кода, которые потерпевшие непосредственно сообщают мошенникам, представившимся сотрудниками банка, по телефону лично либо пройдя по указанной ими ссылке: в целях якобы получения материальной помощи от кредитных организаций, под предлогом перевыпуска банковской карты, воспрепятствования доступа посторонних в личный кабинет, возврата несанкционированно списанных денежных средств, получения предоплаты за товары и услуги, размещённые ими на сайтах продаж в сети Интернет, и т.д.

2. Склонение потерпевшего от имени якобы банка к оформлению «встречных» кредитов под предлогом пресечения оформления кредита на его имя без его ведома с последующим переводим полученных средств на «безопасные счета» (абонентские номера операторов сотовой связи).

3. Склонение потерпевшего представившимся сотрудником банка к обналичиванию банковских карт под предлогом предотвращения мошеннических действий и переводу средств на «безопасные счета».

4. Требование 100-процентной безналичной предоплаты за товары и услуги, информация о которых размещена на сайтах в сети Интернет («Авито», «Юла», «ВКонтакте», «Блаблакар» «Инстаграм» сайты-двойники по продаже ж/д и авиабилетов, бронирование мест в отелях, санаториях, доставка еды и т.д.), после чего связь с продавцом теряется.

*Стоит отметить, что указанная схема мошеннических действий активизировалась в истекшем периоде 2022 года, например:*

*В середине феврале 2022 года неустановленное лицо, используя сервис объявлений «Юла» и сотовый телефон, убедило жителя одного из населенных пунктов Кондинского района в ходе переписки по социальной сети WhatsApp осуществить 2 онлайн-перевода по 2500 руб. с банковской карты Сбербанка на расчетный счет другого банка (при этом причинив заявителю значительный материальный ущерб) под предлогом покупки товара, выставленного на продажу через сервис объявлений «Юла».*

*Другой пример - в конце январе 2022 года житель Кондинского района оставил заявку на заказ двигателя и моторного масла в интернет-магазине ООО «КлючАвто», расположенного в г.Санкт-Петербурге.*

*1 февраля 2022 года на телефон потерпевшего поступил звонок с неизвестного номера от менеджера вышеуказанного магазина с целью информирования о необходимости произвести предоплату за заказанный товар. В результате телефонных переговоров потерпевший перевел со своего телефона с помощью приложения «Сбербанк онлайн» денежные средства в размере 89 500 руб..*

*3 марта у потерпевшего состоялся еще одни телефонный разговор с «менеджером», в ходе которого последний убедил потерпевшего в необходимости оплаты второй половины за заказанный товар, так как двигатель застрял на таможне. В результате явных мошеннических действий житель Кондинского района перевел преступникам еще 90 000 руб.*

*Таким образом, потерпевшему был причинен значительный материальный ущерб в размере 179 500 руб.*

5. Предоставление после 100-процентной предоплаты товаров, не соответствующих заявленному описанию, качеству комплектности и т.д.

6. Склонение потерпевшего к оплате комиссии, страхования, услуг курьера и т.д., под предлогом якобы оказания банковским работником помощи в получении кредита.

7. Направление просьбы о займе денежных средств посредством взлома страниц знакомых на сайтах в сети Интернет.

8. Создание сайтов-двойников с размещениемна них информации о продаже ж/д и авиабилетов, бронирования гостиниц, продаже товаров и т.д.

9. Склонение потерпевшего к оформлению кредитов под предлогом получения дополнительного дохода от инвестиционных вложений с последующими переводами кредитных средств на счета «инвесторов».

10. Склонение потерпевшего представившимся сотрудником правоохранительных органов (МВД, ФСБ) к передаче (переводу) денег под предлогом использования их для разоблачения мошенников.

**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.**

**Такое стало возможным в результате излишней доверчивости граждан к информации от незнакомых лиц, поспешности в принятии решений, личной безответственности, жаждылегкой наживы.**

**В целях профилактики фактов мошенничества и дистанционного хищения денежных средств следует уяснить следующее.**

1. Банки не оказывают услуги посредством телефонной связи.

2. Перевод денежных средств на незнакомые реквизиты недопустим. Обращение друзей и знакомых через социальные сети с просьбой о заимствовании денежных средств – это давно применяемая схема мошенничества.

3. Осуществляя 100-процентную предоплату за оказание тех или иных услуг, приобретение товаров, вы должны быть уверены в надёжности продавца и отдавать себе отчёт о потенциальном риске быть обманутым в такой ситуации. Ни в коем случае не оплачивать товар в сети интернет по предоставленным продавцом или лицом, оказывающим услуги,**ссылки на оплату**, пройдя по которой нужно вводить реквизиты банковской карты («Авито», «Юла», «Дром», «БлаБлаКар»).

4. Пользоваться проверенными сайтами и помнить о том, что злоумышленники создают сайты-двойники, внося незначительные изменения в наименования сайтов добропорядочных организаций.

5. При принятии решения заняться торгово-биржевой или инвестиционные деятельностью, в обязательном порядке необходимо проверять правовой статус инвестиционной компании на сайте ЦБ РФ в разделе «Проверить участника финансового рынка» (по ИНН или ОГРН, а не по наименованию компании).По законодательству РФ профессиональная деятельность на финансовом рынке осуществляется на основании лицензии (ст.39 Федерального закона от 22.04.1996 № 39-ФЗ «О рынке ценных бумаг»).

6. Для разоблачения мошенников, раскрытия каких – либо преступлений сотрудники правоохранительных органов не используют финансовые средства граждан.

Отдел общественной безопасности администрации Кондинского района