Приложение
к исх. от _____ 2021 №_____

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 2 квартала 2021 года

По информации Управления Министерства внутренних дел Российской Федерации по Ханты-Мансийскому автономному округу – Югре (далее – автономный округ) во втором квартале 2021 года органами внутренних дел автономного округа зарегистрировано 107 сообщений о преступлениях, предусмотренных ст.ст.158, 159 УК РФ и связанным с дистанционным хищением (завладением) денежных средств с банковских карт граждан, совершённых в отношении государственных и муниципальных служащих, сотрудников и работников бюджетной сферы.

Наибольшее количество таких преступлений зарегистрировано в г.Сургуте (24), г.Ханты-Мансийске (20), г.Нижневартовске (19), Сургутском районе (8).

В г.Нягани зарегистрировано 6 таких преступлений, 5 – в Советском районе, по 4 – в г.Нефтеюганске и Кондинском районе, 3 – в г.Радужном, по 2 – в Березовском и Октябрьском районах, по 1 – в г.Когалыме, г.Лангепасе, г.Мегионе, г.Пыть-Яхе, г.Урае, г.Югорске, Белоярском, Нефтеюганском и Нижневартовском районах.

В г.Покачи и Ханты-Мансийском районе в указанный период таких преступлений не зарегистрировано. Одна попытка на совершение преступления мошенникам не удалась в г.Урае по причине бдительности гражданина.

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.

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.

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 размещением на 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».

Таким образом, в абсолютном большинстве случает 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, жажды легкой 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»).