УМВД России по Ханты-Мансийскому автономному округу - Югре

УПРАВЛЕНИЕ МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ГОРОДУ СУРГУТУ (УМВД России по г.Сургуту)

ул. Маяковского, 19, Сургут, 628403

27.04.2022 № 22-2/26220

Главному врачу БУ ХМАО-Югры «Сургутская городская клиническая поликлиника № 1»

М. Н. Слепову
г. Сургут, ул. Сибирская, д.14/2

О направлении информации

Уважаемый Максим Николаевич!

В связи с участившимися случаями дистанционного мошенничества данный вид преступления находиться на особом контроле как в УМВД России по ХМАО-Югре так и в целом в МВД Российской Федерации и вызывает широкий общественный резонанс. С каждым днем злоумышленники придумывают новые способы и схемы мошенничества, в связи с чем, увеличиваются обращения граждан по различным фактам мошенничества.

Основными видами мошенничества, на которые попадаются граждане, являются:

1. Приобретение товара, либо заказ услуги через группы социальных сетей «Вконтакте», где гражданину предлагается сначала внести стопроцентную предоплату, а после он получит свой товар, либо запись на необходимую услугу.

2. Приобретение товара через сайты бесплатных объявлений («Авито», «Юла»), где злоумышленник поясняет, что товар есть в наличии, однако для его получения необходимо выслать либо стопроцентную предоплату, или половину стоимости товара, если указана большая сумма оплаты, может выслать гражданину, по просьбе последнего, его фото, либо товарно-транспортную накладную о том, что товар действительно находится в одной из транспортной компании с чеком об оплате, так же злоумышленник поясняет, о том, что он хочет приобрести товар гражданина, либо получить его услугу, однако ввиду того, что он переживает за то, что гражданин может продать товар, либо то, что злоумышленник находится в настоящее время далеко, и поясняет, что хотел бы перевести денежные средства на банковскую карту гражданина, однако чтобы это сделать гражданин

должен назвать номер банковской карты, срок ее действия, cvc код, а в последующем пароль, который поступит гражданину на сотовый телефон. При этом убеждая гражданина в том, что это абсолютно безопасно и в качестве примера может перевести какую-нибудь сумму денег, либо сделать видимость по переводу денежных средств, где в смс - сообщении поступившим на сотовый телефон гражданина будет отражаться указанная информация, в основном злоумышленник, скидывает ссылку якобы «система безопасных платежей», где необходимо ввести реквизиты банковской карты, с последующем введением кода из смс-сообщения.

3. Поиск товара через поисковые системы сети Интернет, где гражданин попадает не на официальный сайт продажи товара, а на фишинговый (дубликатный) сайт, где размещается одинаковая информация, размещаемая и на официальном сайте, с изменением расчетного счета перечисления денежных средств, а также контактных данных.

Чтобы не попасться на уловки злоумышленников, ***необходимо помнить***, что нельзя говорить мошеннику номера своих банковских карт, не перечислять предоплату, пока не увидите товар лично, не поддаваться дешевой цене за товар, не осуществлять покупку на не проверенных сайтах, перед покупкой обратить внимание на отзывы, посмотреть дату создания сайта.

Запомните, не отправляйте предоплату, ни в каких суммах по не проверенным сайтам и не соблазняться заниженной ценой товара

Прошу в обратном письме предоставить ведомость (дата, ФИО, подпись) об ознакомлении сотрудников структурного подразделения с вышеуказанной информацией.

Врио начальника С.Л. Успенский

Исп.: Хафизов И.И.
76-19-80