ЛЕКЦИОННЫЙ МАТЕРИАЛ – ПРОФИЛАКТИКА МОШЕННИЧЕСТВА

Проблема дистанционных преступлений для нашего региона, как и для всей страны в целом, не теряет своей актуальности. Несмотря на постоянную профилактическую работу, с начала 2021 года зарегистрировано почти 2,5 тысячи дистанционных мошенничеств и краж с банковских счетов граждан. Общая сумма ущерба превысила 278 миллионов рублей.

1. Наиболее частым способом совершения преступлений является звонок от лица службы безопасности банка. Потерпевшему сообщают, что с его счета совершена попытка несанкционированного списания денежных средств. Для предотвращения операции предлагают продиктовать номера банковской карты и коды безопасности, приходящие в СМС-сообщениях. Эти сведения строго конфиденциальны! После их разглашения преступники получают доступ к вашему банковскому счету!

В последнее время вторым по частоте стал звонок от имени службы безопасности банка с сообщением о попытке третьих лиц оформить на Ваше имя кредит. Чтобы это предотвратить, предлагается срочно оформить такой же кредит самому, а денежные средства обналичить и перевести на т.н. «безопасный» счет. Несмотря на очевидную абсурдность ситуации, огромное количество потерпевших идут на поводу у мошенников, оформляют многомиллионные займы и переводят их на номера интернет-кошельков или мобильных телефонов. Печальный рекорд этого года – семейная пара перевела мошенникам почти 8 миллионов рублей.

ЗАПОМНИТЕ! Службы безопасности банков никогда не звонят клиентам с сообщениями о проблемах со счетом. Любой подобный звонок – дело рук мошенников. Все вопросы, связанные с обслуживанием вашей банковской карты, необходимо решать только по телефону службы технической поддержки, который расположен на оборотной стороне любой банковской карты. Он бесплатный и круглосуточный. Никогда и никому не сообщайте номера и коды безопасности банковских карт!

2. Покупки в сети Интернет. Чаще всего преступления совершаются с использованием сервисов бесплатных объявлений (авито, юла и т.д.) Причем жертвой преступления может стать как покупатель, так и продавец.

- При покупке вещи в сети интернет необходимо помнить, что любой дистанционный перевод денежных средств незнакомому человеку потенциально опасен. Вы не можете гарантировать, что он выполнит свою часть сделки. То же касается и непроверенных интернет-магазинов. Вы можете не получить оплаченную вещь, либо получить совсем не то, что заказывали. Пользуйтесь проверенными сервисами и системами безопасного расчета.

- При размещении объявления о продаже вещи человеку поступает звонок от потенциального покупателя. Он сообщает, что готов приобрести данную вещь и предлагает внести предоплату. Для перечисления денег просит сообщить данные банковской карты, включая код проверки подлинности карты (CVV2,CVC2, CVP2) и коды безопасности из СМС-сообщений. После передачи

конфиденциальных сведений со счета потерпевшего происходит списание денежных средств.

3. Большое число преступлений совершается через социальные сети. Чаще всего страницы пользователей взламываются, либо копируются. После чего кругу «друзей» рассылаются сообщения с просьбой дать денег в долг. Никогда не перечисляйте деньги после просьб в соцсетях. Обязательно созвонитесь с человеком ЛИЧНО.

4. Еще одна преступная схема – предложения от имени известных банков принять участие в розыгрыше и гарантированно получить денежный приз. Для этого необходимо заполнить специальную форму, куда, помимо персональных сведений, необходимо внести конфиденциальную информацию о номерах, кодах безопасности банковской карты, а также ввести код из СМС-сообщений. После разглашения данных конфиденциальных сведений со счета потерпевшего списываются денежные средства.

5. Не устанавливайте на телефон неизвестные мобильные приложения. Среди них могут оказаться как вирусные программы, так и сервисы по удаленному управлению телефоном. Если у вас подключены системы дистанционного управления финансами, данные вредоносные программы получат доступ к ним и к вашим сбережениям. Чтобы обезопасить себя не переходите по сомнительным ссылкам в СМС и ММС сообщениях, не устанавливайте программы, назначение которых вам не понятно, используйте лицензионное антивирусное программное обеспечение!

Будьте бдительны. Не позволяйте мошенникам обманывать вас.

Отдел информации и общественных связей
УМВД России по Архангельской области

2021 год