ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ!

УМВД России по Архангельской области предупреждает об активизации телефонных и интернет мошенников.

1. Никогда и никому не сообщайте пин-код банковской карты, пароль от мобильного- и интернет-банка, трехзначный код на обороте карты, коды из СМС.

2. Сотрудники банков никогда не запрашивают информацию о банковской карте. Любой подобный звонок, даже если он совершается якобы с официального номера банка, – дело рук мошенников!

3. Если Вам звонят и сообщают о проблемах с Вашим счетом, или попытках оформить на Вас кредит, положите трубку. Сами наберите номер телефона банка, который указан на обороте карты, и выясните, все ли в порядке с Вашими деньгами.

4. Совершая покупки или продажи в Интернете, на сайтах с бесплатными объявлениями или в интернет-магазинах, будьте осторожны. Не сообщайте лишние данные. Для перевода денег достаточно номера телефона или номера карты.

5. Не переходите по ссылкам в сообщениях от незнакомых людей, которые пришли к Вам по почте, в соцсетях или в СМС.

6. Знакомый в социальных сетях просит перевести ему деньги? Обязательно перезвоните человеку, от лица которого поступает просьба. Его аккаунт может быть взломан!

7. Не устанавливайте на мобильные телефоны и компьютеры приложения из непроверенных источников. Есть программы, позволяющие удаленно управлять вашим телефоном или компьютером! Используйте лицензионное антивирусное программное обеспечение.

8. Получили сообщение о подарке от банка или беспроигрышной лотерее? Для получения приза просят ввести данные карты? Это обман! Никому не сообщайте конфиденциальную информацию о номерах и кодах банковских карт.

9. Нашли в сети Интернет информацию о возможности заработать на курсах акций? Будьте бдительны! Вас могут обмануть! Пользуйтесь услугами официально зарегистрированных брокерских организаций.

10. В любой ситуации сохраняйте бдительность и критическое мышление! Не позволяйте мошенникам обманывать Вас.

Если вы стали жертвой преступления, незамедлительно обращайтесь в полицию по номерам телефонов 02 (102) или 112.

ЛЕКЦИОННЫЙ МАТЕРИАЛ – ПРОФИЛАКТИКА МОШЕННИЧЕСТВА

Проблема дистанционных преступлений для нашего региона, как и для всей страны в целом, не теряет своей актуальности.

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.

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

2022 год