Приложение № 1
к Приказу №

УМВД России по Архангельской области
Памятка по мошенничествам и кражам

КАК УБЕРЕЧЬСЯ ОТ ДИСТАНЦИОННЫХ МОШЕННИЧЕСТВ И ХИЩЕНИЙ ДЕНЕЖНЫХ СРЕДСТВ С БАНКОВСКИХ КАРТ

Одной из причин совершения преступлений, связанных с мобильным мошенничеством, является постоянное развитие и совершенствование компьютерной техники, сети Интернет, их повсеместное распространение, повышение уровня их доступности для различных слоев населения.

Зачастую, мошенничеством такого типа занимается несколько лиц, некоторые из них могут даже отбывать наказание в исправительных учреждениях.

Основные схемы дистанционных мошенничеств:

Во многих случаях преступление проводится по следующим схемам:

• Неизвестное лицо при помощи мобильного телефона с абонентским номером, как правило с «московским» кодом, например, +74953696998 (+74993696998) осуществляет звонок потерпевшему, сообщает, что является сотрудником службы безопасности (работником) ПАО «Сбербанк России» (любого другого банка), а также, что с банковской карты потерпевшего были совершены незаконные операции по снятию или переводу денежных средств и/или банковская карта заблокирована, в связи с чем потерпевшему в срочном порядке необходимо все (часть) денежных средств со счета своей банковской карты перевести на счет только что открытой на имя потерпевшего банком банковской карты, после чего потерпевший в своем личном онлайн – кабинете и или через терминал переводит денежные средства со своей банковской карты на номер банковской карты, указанной звонившим сотрудником ПАО «Сбербанк России», после чего деньги переводятся неизвестному, номер телефона, с которого звонил якобы сотрудник банка, выключается.

• Размещения на интернет-сайте «AVITO», других интернет-сайтах объявлений с ложной информацией. На сайтах выкладываются объявления с информацией о продаже мебели, телефонов, снегоходов, автомобилей, запчастей и т.д. В объявлении указывается контактный номер сотового телефона мнимого владельца. При установлении контакта с продавцов, продавец просит внести предоплату (иногда 100 %) за продаваемый товар и перевести денежные средства на счет банковской карты или абонентский номер, привязанный к банковской карте, после чего обещает выслать или передать интересуемый покупателя товар. В дальнейшем получает денежные средства за товар и скрывается от покупателя, блокируя его номер телефона, товар покупателю не направляется.

• Неизвестное лицо, «взломав» профиль (личную страницу) в социальной сети «Вконтакте» («Инстаграмм», «Одноклассниках» и т.д.) знакомого

(знакомой, друга, супруги) потерпевшего, в ходе переписки с потерпевшим от лица якобы его знакомого, просит одолжить денег на непродолжительное время, ссылаясь на трудное финансовое положение, на согласие потерпевшего помочь знакомому, неизвестное лицо просит потерпевшего перевести денежные средства на абонентский номер или банковскую карту, после перевода денежных средств потерпевший связывается со своим знакомым для подтверждения перевода, но в ответ слышит, что его знакомый на самом деле никаких денежных средств в долг не просил, а его профиль в социальной сети взломан.

• Родственник в беде. Схема, которая работает как на мобильных, так и на стационарных телефонах. Когда вы отвечаете на звонок, собеседник говорит, что он ваш родственник и рассказывает историю о его задержании полицией за совершение преступления. После этого трубку берет другой человек, представляется сотрудником полиции и излагает свои требования взамен на некоторую сумму денег (как правило деньги необходимы для прекращения только что возбужденного уголовного дела в отношении родственника, несоставления заявления о преступлении в отношении родственника). Часто деньги нужно перевести на продиктованный якобы сотрудником полиции абонентский номер или привести в определенное место и/или передать через человека. После перевода денежных средств, телефон с которого звонил родственник и сотрудник полиции оказывается выключенным, а позже перезвонивший родственник сообщает, что никаких преступлений он не совершал и в полиции не оказывался.

Основные схемы хищений денежных средств с банковских карт:

• Неизвестное лицо при помощи мобильного телефона с абонентским номером, как правило с «московским» кодом, например, +74953696998 (+74993696998) осуществляет звонок потерпевшему, сообщает, что является сотрудником службы безопасности (работником) ПАО «Сбербанк России» (любого другого банка), а также, что с банковской карты потерпевшего были совершены незаконные операции по снятию или переводу денежных средств и/или банковская карта заблокирована, в связи с чем работнику банка для предотвращения незаконных операций (возврата денежных средств) необходимы реквизиты банковской карты потерпевшего. Получив от потерпевшего коды и реквизиты банковской карты, злоумышленник, используя вредоносную программу, похищает денежные средства со счета карты.

• Неизвестное лицо при помощи мобильного телефона с абонентским номером, как правило с «московским» кодом, например, +74953696998 (+74993696998) осуществляет звонок потерпевшему, сообщает, что является сотрудником службы безопасности (работником) ПАО «Сбербанк России» (любого другого банка), а также, что потерпевший стал победителем в акции проводимой ПАО «Сбербанк России», ему от банка гарантированы денежные средства в качестве приза, в связи с чем сотруднику банка необходимы

реквизиты банковских карт потерпевших для того, чтобы перевести денежные средства. Получив от потерпевшего коды и реквизиты банковской карты, злоумышленник, используя вредоносную программу, похищает денежные средства со счета карты, приз от ПАО «Сбербанк России» является легендой.

• Неизвестное лицо, «взломав» профиль (личную страницу) в социальной сети «Вконтакте» («Инстаграмм», «Одноклассниках» и т.д.) знакомого (знакомой, друга, супруги) потерпевшего, в ходе переписки с потерпевшим от лица его знакомого, сообщает потерпевшему о получении бонусов (денежных средств) от ПАО «Сбербанк России», которые переводятся на счета банковских карт, в связи с чем сотруднику банка необходимы реквизиты банковских карт потерпевших для того, чтобы осуществить переводы. Получив от потерпевшего коды и реквизиты банковской карты, злоумышленник, используя вредоносную программу, похищает денежные средства со счета карты, приз от ПАО «Сбербанк России» является легендой.

Как избежать?

Для того чтобы не потерять свои деньги, обратите внимание на следующие рекомендации:

• Не принимайте быстрых решений. Помните, что главная цель преступников – сбить вас с толку и не дать времени на обдумывание ситуации.

• Обязательно проверьте информацию, которую вам предоставили. В случае с родственниками, позвоните на их телефоны или свяжитесь с окружающими их людьми или сотрудниками. В случае если речь идет об операторе или банке – позвоните по горячему номеру. Обычно номера банка указаны на банковских картах с обратной стороны.

• Не сообщайте преступникам личные сведения, номера своих банковских карт, коды доступа, смс - сообщения которые поступают к вам на телефон иным лицам.

• Ни в коем случае не перезванивайте на незнакомые номера и не вводите предложенных подозрительных кодов.

УМВД России по Архангельской области убедительно просит жителей Архангельской области проявлять бдительность!