

Алгоритм действий граждан, при получении ими звонков или сообщений мошеннического характера

1. Если вы получили звонок (на мобильный или стационарный телефон) от якобы близкого родственника или знакомого с информацией о том, что он попал в неприятную ситуацию, ему грозит привлечение к уголовной ответственности и предлагается дать взятку сотруднику правоохранительных органов, готовому урегулировать вопрос:

- задайте "родственнику" наводящие вопросы, ответы на которые знаете Вы оба, либо попросите описать себя;

- спросите, в какое отделение полиции доставлен родственник. Выясните, действительно ли Ваш родственник находится там и кто занимается этим делом.

- перезвоните на мобильный телефон своего родственника. Если он отключен, очертите круг лиц, которые могут знать о его местонахождении (коллеги по работе, друзья, близкие лица), свяжитесь с ними для уточнения информации.

- обязательно позвоните по телефону 02 и сообщите дежурному сотруднику полиции о произошедшем.

2. При поступлении на мобильный телефон СМС – сообщения от якобы знакомых с просьбой положить на их счет деньги, либо о том, что Ваша банковская карта заблокирована:

- ни в коем случае не звоните на мобильные номера указанные в sms сообщении к примеру « инф. по телефону +79815265685»;

- перезвоните своим родственникам от чьего имени пришло СМС и узнайте о том, отправляли ли они Вам сообщение.

3. В случае если Вам перезвонили неизвестные и представившись работниками банка сообщили о том, что Ваша карта заблокирована, задайте следующие вопросы:

- знает ли он номер заблокированной карты;

- в каком отделении банка и когда была открыта банковская карта.

Если звонивший не сможет ответить хотя бы на один вопрос, знайте это **мошенники**.

Незамедлительно позвоните по телефону 02 и сообщите дежурному сотруднику полиции о произошедшем.

Отдел полиции по обслуживанию Ковдорского района

УМВД России по Мурманской области предупреждает граждан об участившихся случаях осуществления переводов денежных средств с использованием устройств мобильной связи (смартфоны, телефоны, планшеты) без согласия их владельцев.

Несанкционированные операции, как правило, осуществляются вследствие заражения устройств мобильной связи вредоносными программами (в том числе вирусами), через спам-рассылку сообщений (sms-сообщений, сообщений электронной почты), содержащих ссылки на внешние ресурсы, или при переходе пользователя устройства мобильной связи по ссылкам на ресурсы сети Интернет. При переходе пользователя по таким ссылкам вирус устанавливается на устройство мобильной связи.

Вредоносные программы могут обладать различными возможностями, в т.ч.:

- формируют и отправляют от имени пользователя мобильного устройства распоряжения на перевод денежных средств, в том числе в виде sms-сообщений на «короткие номера»;
- формируют и отправляют от имени пользователя мобильного устройства распоряжения на перевод денежных средств с использованием приложений ДБО и иных приложений, предназначенных для оплаты товаров и услуг;
- перехватывают одноразовые коды подтверждения, приходящие на мобильное устройство в целях дополнительного подтверждения операции.

Вирусная программа обеспечивает доступ злоумышленников к сервису «мобильный банк» и автоматически отправляет команды в банк о списании денег со счета. При этом происходит блокировка sms-сообщений о движении денежных средств и владелец карты не может своевременно обнаружить исчезновение денег.

УМВД России по Мурманской области предупреждает граждан о необходимости быть предельно внимательными при получении sms-сообщений с незнакомых телефонных номеров. Не следует открывать сообщения, содержащие ссылки на сайты в сети Интернет. Установку приложений для смартфонов рекомендуется производить только с официальных ресурсов.

Установка на мобильное устройство лицензионного антивирусного программного обеспечения позволит защищаться от всех типов вредоносного программного обеспечения, используемого мошенниками для совершения киберпреступлений.

Еще одним способом защититься от несанкционированного списания денег является подключение услуги «Мобильный банк» к отдельной сим-карте, которая будет использоваться в мобильном телефоне бюджетной модели без возможности выхода в сеть Интернет.

