ПАМЯТКА

для сотрудников, задействованных на профилактических мероприятиях по предупреждению преступлений совершаемых в сфере информационно — телекоммуникационных технологий.

К наиболее распространённым способам совершения преступлений с использованием информационно-телекоммуникационных технологий можно отнести следующие:

- мошенники звонят гражданам, представляясь сотрудниками банков, называя их по фамилии, имени и отчеству, просят сообщить данные банковских карт (номер, CVC(CVV), PIN-коды и т.п.) для предотвращения якобы несанкционированного списания денежных средств либо оформления кредита. Используя эти сведения, получают удаленный доступ к личному кабинету клиента банка и переводят деньги без ведома собственника. При этом, преступники могут использовать программы подмены телефонных номеров, в связи с чем номер входящего звонка определяется у клиента как номер банка;

- распространены и способы хищения с использованием таких популярных сервисов как «Юла», «Avito» и т.д. вводя гражданина в заблуждение относительно своего намерения приобрести или продать товар, в ходе телефонных разговоров злоумышленники узнают реквизиты банковской карты потерпевшего, при помощи которых списывают денежные средства со счета. Зачастую предлагается перейти по ссылкам для перевода денежных средств, после чего «мнимый продавец» не предоставляет оплаченный товар и не выходит на связь;

- массовые рассылки SMS-сообщений, например содержания: «Ваша карта заблокирована. Для разблокировки необходимо позвонить по номеру…». Граждане, вместо того, чтобы сразу обратиться в свой банк для проверки данной информации, перезванивают по указанному в SMS-сообщении номеру и в ходе разговора передают мошенникам информацию о банковских реквизитах, после чего осуществляется незаконное списание денежных средств;

- мошенники также взламывают аккаунты граждан в социальных сетях, электронную почту и от имени пользователя рассылают гражданам, сведения о которых имеются в контактах данного лица, просьбы о займе денежных средств. В результате деньги поступают на счет мошенника.

В связи с вышеизложенным для предотвращения совершения мошеннических действий необходимо действовать по следующему алгоритму:

- в случае получения звонка или сообщения о материальной помощи для знакомых или родственников, не принимать решение сразу, следует проверить достоверность полученной информации, связаться с указанными лицами;

- ни при каких обстоятельствах не сообщать трехзначный код на оборотной стороне Ваших банковских карт, личные сведения, смс пароли и т.д.;

- никогда не выполнять действия с банкоматом «под диктовку» в ходе телефонного разговора, незамедлительно прервать разговор;

В случае если мошенники представляются сотрудниками банков, помните, что сотрудники банка никогда:

- не предлагают установить программы или приложения на мобильные телефоны удаленного доступа и разрешить им подключение к Вашему устройству для технической поддержки;

- перевести денежные средства на безопасный счет;

- включить переадресацию на телефоне, для совершения звонков от имени гражданина в банк.

УУР МВД по Республике Хакасия