Берегитесь мошенников!

Ранее такие статьи неоднократно появлялись в средствах массовой информации, но большинство людей считает, что все происходит с другими, а с ними не случится, но преступления связанные с телефонным мошенничеством, распространены как никогда сейчас.

В современных условиях очень сложно отследить мошенника. Информационные технологии развиты настолько, что путем манипуляций можно выманить деньги у доверчивых граждан даже находясь в колонии или в другой стране. Обналичить средства тоже не составляет труда. Киви-кошелек, банкоматы или счета сотовых операторов позволяют мошенникам фактически безнаказанно пользоваться выкачанными деньгами.

**ОМВД России по Добринскому району напоминает гражданам о правилах безопасности при пользовании банковскими картами, услугами «Мобильный банк» и «Банк Онлайн».**

Современные банковские технологии позволяют значительно упростить проведение платежей, денежных переводов, расчетов при покупках и т.д. Их применение при соблюдении особых правил со стороны пользователей безопасно и надежно.

Так, есть ряд простых руководств, которым должны следовать владельцы банковских карт:

• ПИН-код карты должен быть известен только владельцу карты;

• ни при каких обстоятельствах банковская карта не должна использоваться третьими лицами, в том числе родственниками;

• в торговых точках, кафе платежные операции по карте должны проводиться в присутствии владельца;

• Интернет-покупки необходимо совершать только на известных, проверенных  ресурсах (или использовать электронные кошельки).

**При работе в системе «Банк Онлайн» необходимо помнить о следующих мерах безопасности.**

• идентификатор и пароль для входа в систему должен быть известен только пользователю;

• не вводить пароль для отмены или аннулирования операций. Пароли на отмену или аннулирование операций могут запрашивать только мошенники. Сотрудники банков никогда не звонят клиентам и не просят отменить/аннулировать операции;

• не вводите свой номер телефона, номер паспорта и другие данные при подтверждении операций или входе в Банк Онлайн;

• внимательно читать SMS-сообщения, всегда проверять реквизиты операции. При получении сообщения с операцией, которая не совершалась, ни при каких обстоятельствах не вводить пароль.

Пользователям «Мобильного банка» необходимо:

• при утрате мобильного телефона (устройства), на который подключена услуга «Мобильный банк» или на которое установлено мобильное приложение Банк Онлайн следует срочно обратиться к своему оператору сотовой связи для блокировки SIM-карты и в Контактный Центр Банка для приостановки действия услуги «Мобильный банк» и/или «Банк Онлайн»;

• при смене номера телефона, на который подключена услуга «Мобильный банк» обратиться в любой офис банка и оформить заявление на отключение услуги «Мобильный банк»;

• установите на телефон антивирус и своевременно его обновлять. Кроме того, есть ряд рекомендаций по защите от СМС и e-mail мошенничества. Мошеннические СМС-сообщения, как правило, информируют о блокировке банковской карты, о совершенном переводе средств или содержат другую информацию, побуждающую перезвонить на указанный в СМС-сообщении номер телефона для уточнения информации. Затем мошенники представляются сотрудниками службы безопасности, специалистами службы технической поддержки и в убедительной форме предлагают срочно провести действия по разблокировке карты, по отмене перевода и т.п., в зависимости от содержания СМС-сообщения. В случае получения подобных СМС-сообщений банк настоятельно рекомендует:

• не перезванивать на номер телефона, указанный в СМС-сообщении;

• не предоставлять информацию о реквизитах карты (номере карты, сроке ее действия, ПИН-коде, CVV2/CVC2 коде, контрольной информации по карте), или об одноразовых паролях, в т.ч. посредством направления ответных СМС-сообщений;

• не проводить через банкоматы и иные устройства самообслуживания никакие операции по инструкциям, полученным по телефону.

Соблюдение элементарных правил безопасности позволит Вам защитить себя от мошенничества. Главное следовать им в повседневной жизни.