Профилактика дистанционного мошенничества.

Дистанционное мошенничество, преимущественно, совершается следующими способами:

- Потерпевшие сообщают мошенникам реквизиты и пароли доступа к операциям по счету посредством поступившего им СМС-сообщения, что приводит к хищению денежных средств.

- Значительную распространённость имеют преступления, совершенные с использованием высоких технологий, то есть в сети Интернет, в том числе объявления о продаже и рассылки вирусных ссылок в социальных сетях.

Анализ преступлений, совершенных дистанционным способом, показывает, что одним из признаков подготавливаемого или совершаемого преступления телефонного мошенничества является, когда мошенники выступают в роли «сотрудников службы безопасности банков» и в ходе телефонного разговора получают информацию по банковской карте (номер банковской карты, а также CV-код).

Дальнейшим основным фактором является получение злоумышленниками разового пароля (в виде СМС-сообщения), который поступает на абонентский номер, привязанный к банковской карте. Держатель банковской карты сообщает разовый пароль мошенникам, тем самым предоставляет доступ к денежным средствам.

Уважаемые граждане, в целях пресечения и противодействия преступных намерений и действий мошенников, ОМВД России по Ташлинскому району информирует Вас о том, что в настоящее время активно распространен вид телефонного мошенничества, злоумышленники звонят и представляются сотрудниками служб безопасности банков, после чего дезинформируют о том, что с карты осуществляются попытки несанкционированного списания денежных средств.

Основные моменты:

1. Не диктовать пароли из смс-сообщений

2. При поступлении подобного рода звонка, незамедлительно завершить разговор, и перезвонить по официальному телефону банка.

3. В случае утери телефона незамедлительно сообщите в банк о приостановлении (блокировке) имеющихся на счетах сбережений.