**Главе Октябрьского муниципального района**

**и главам сельских поселений Октябрьского района**

**Осторожно, мошенники!**

 Текст

Важнейшая проблема, с которой сталкиваются многие граждане – это дистанционное мошенничество, связанное с получением мошенниками удаленного доступа к банковской карте и интернет-мошенничеством. Довольно часто мошенники выдают себя за сотрудников банка.

Помните! При звонке клиенту сотрудник банка никогда не просит сообщить ему реквизиты карты и совершать какие-либо операции с картой.

Мошенниками могут быть запрошены у жертвы следующие данные:

* ПИН-код карты
* Код безопасности (CVV2 или CVC2)
* Одноразовый пароль банка для подтверждения оплаты онлайн

Ни в коем случае не сообщайте ПИН-код, код безопасности или одноразовый пароль третьим лицам!!!

Одним из самых распространенных видов интернет-мошенничества является так называемый «фишинг». Мошенники совершают определенные действия, направленные на получение доступа к денежным средствам на банковской карте потенциальной жертвы, при помощи почтовых рассылок от лица банка, содержащих в себе ссылки на страницы, являющиеся точными копиями официальных сайтов, на которых предлагается ввести данные карты для возможности дальнейшего ее использования.

Распространенным способом мошенничества является мошенничество в социальных сетях. Мошенники взламывают персональную страницу пользователя в социальных сетях или мессенджере и отправляют сообщения с просьбой помочь и срочно перевести денег.

Будьте осторожны!

Прокурор района

советник юстиции А.И. Бутрик