Как не стать жертвой кибермошенников!

На территории Гродненской области и республики в целом значительно увеличилось количество преступлений, совершаемых путем использования компьютерной техники, в том числе хищений. На территории Гродненского района также имеет место совершение преступлений данной категории.

Совершению киберпреступлений способствует активизация расчетов граждан с использованием компьютерной техники, популярность приобретения товаров на Интернет-площадках, цифровая неграмотность и, самое главное - излишняя доверчивость граждан.

В большинстве случаев последние сами предоставляют злоумышленникам все сведения о себе, реквизиты банковских карточек либо добровольно следуют инструкциям злоумышленников. Как результат - списание со счетов граждан значительных денежных сумм.

Наиболее распространенным видом киберпреступлений является так называемый «ВИШИНГ». Гражданам звонят якобы из банка (сотрудники банка, представители службы безопасности банка), также имели место звонки якобы из органов внутренних дел, и, введя в заблуждение, узнают реквизиты банковских карточек и личные данные, после чего совершается хищение денежных средств.

Еще одним распространенным видом киберпреступлений является «ФИШИНГ», когда гражданам в социальных сетях, мессенджерах, форумах отправляются сообщения якобы от имени друзей, или администрации сайта (как правило, Интернет-площадок по продаже товаров) с вложением «фишинговой ссылки», после открытия которой пользователю предлагается заполнить реквизиты банковской карточки для доставки ранее заказанного товара либо подтверждения платежа. После получения необходимых сведений злоумышленники также совершают хищение денежных средств.

Чтобы не стать жертвой кибермошенников, необходимо, НИКОМУ, в том числе лицам, якобы позвонившим «из банка», «милиции» и др., не сообщать свои персональные данные, реквизиты банковской карточки (номер, имя и отчество, срок действия, cvc-код, указанный с обратной стороны карты), коды из смс-уведомлений банка, клиентом которого Вы являетесь.

При размещении объявлений о продаже товара на торговых Интернет-площадках (к примеру, «куфар бай» и др.), покупке товаров на таких площадках: совершайте все действия (общение, перевод денег и др.) только на торговой площадке; по возможности инициируйте непосредственно личное («лицом к лицу») общение с потенциальным

покупателем (продавцом) товара; не переходите по ссылкам, которые Вам присылают в WhatsApp, Viber и других мессенджерах;

- при общении, НИКОМУ не сообщайте реквизиты своей банковской карточки, в т.ч. посредством их ввода в ходе заполнения при переходе по представленным ссылкам (а также путем заполнения представленных электронных форм документов, заявок, предложений об оформлении доставки товара и пр.);

- при поступлении сообщений в мессенджере, социальной сети о блокировке Вашей банковской карточки ни в коем случае не переходите по прикрепленным ссылкам, никуда не пересылайте свои данные. При наличии вопросов, самостоятельно обратитесь в банковское учреждение, в т.ч. по указанному на банковской карточке телефонному номеру.

Выполнение этих простых правил поможет сберечь Ваши финансовые средства, нервы и не стать жертвой кибермошенников.

Также обращаем Ваше внимание на необходимость доверительного общения с детьми на предмет выявления возможных фактов совершения (попыток) в отношении них сексуального насилия, иных противоправных действий посредством общения в мессенджерах, социальных сетях. О ставших известными таких фактах сообщите в Гродненский РОВД.