Как не стать жертвой мошенников в киберпространстве.

На территории Могилевской области и республики значительно увеличилось количество преступлений, совершаемых путем использования компьютерной техники, в том числе хищений.

В частности, по итогам 5 месяцев 2023 г. на территории республики зарегистрировано практически 7 тысяч киберпреступлений, в Могилевской области - 556 (5 месяцев 2022 г.- 476).

В текущем году негативная тенденция увеличения количества киберпреступлений имеет место в г.Могилеве и Бобруйске (на их долю приходится 43% и 25% от общего числа зарегистрированных в регионе преступлений данной категории), а также в 8 районах области. На территории Мстиславского района по состоянию на 28.06.2023 таких преступлений совершено – 11.

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

В большинстве случаев граждане, будучи обманутыми, 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 «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 совершают хищение денежных средств.

Еще одним распространенным видом киберпреступлений является «ВИШИНГ» - гражданам **звонят** якобы из банка или правоохранительных органов (злоумышленники представляются работниками банка, службы безопасности банка либо сотрудниками милиции, следователями и др.) и, введя в заблуждение, узнают реквизиты банковских карточек и личные данные, после чего совершается хищение денежных средств.

Также многочисленны случаи покупки на сайтах с наименованиями, ассоциирующимися как реализующие тот или иной конкретный товар (обувь, бытовая техника, посуда, постельные принадлежности, одежда и др.), когда граждане осуществляют перевод денежных средств продавцу-

мошеннику, который не намеревался предоставлять товар добросовестному покупателю.

Согласно информации управления по противодействию киберпреступности УВД Могилевского облисполкома большинство потерпевших в результате хищений путем использования компьютерной техники - граждане 30 - 50 лет, как правило, женщины, с высшим образованием. Имеют место факты совершения преступлений и в отношении лиц пенсионного возраста.

Чтобы не стать жертвой киберпреступников, 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. Запомните, **НИКТО** без вашего участия не может оформить кредит в банке. **НЕ НАДО** оказывать услугу «якобы службе безопасности банка» по изобличению недобросовестных работников банка- окажетесь без денег, а кредит придется выплачивать **ВАМ**.

При размещении объявлений о продаже товара на торговых Интернет-площадках (к примеру, «Куфар», «АУ БАИ» 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 нервы, финансовые средства, и не стать жертвой киберпреступников.

Прокурор Мстиславского района
старший советник юстиции В.Н. Тривайло