Профилактика мошенничества в сети Интернет

На территории Республики Беларусь, в том числе и в Климовичском районном отделе Следственного комитета Республики Беларусь регистрируется значительное количество преступлений, связанных с совершением мошеннических действий с применением информационно-компьютерных технологий. В настоящее  время основными способами завладения денежными средствами граждан являются фишинг и вишинг.

ФИШИНГ: Мошенники умело подделывают различные интернет-ресурсы, которые имеют услугу онлайн-платежей, например, банковские услуги, торговые площадки, службы доставки и другие. Фишинг предполагает способ, цель которого - завладеть личными данными граждан: реквизитами банковских платежных карт, сеансовыми ключами (кодами из смс), паролями к сервисам, чаще всего к М-банкингу.

ВИШИНГ: Для совершения преступлений мошенники чаще всего используют звонки в мессенджерах«Whatsapp», «Telegram», «Viber». При этом звонящие могут представиться сотрудниками банковских организаций или правоохранительных органов, после чего под различными предлогами убеждают произвести какие-либо действия, например, передать конфиденциальную информацию, в том числе смс-коды, оформить кредит или установить мобильное приложение.

Чтобы не стать жертвой мошенников:

- никому и ни под каким предлогом не передавайте номер банковской карты, срок действия, трехзначный секретный код на обороте, логины и пароли доступа к банкингу, смс-коды от банка.

- не устанавливайтена телефон незнакомые программы и не переводить деньги по указанию, полученному по телефону даже от лиц, представившихся работниками банка или милиции.

- при поступлении звонка в мессенджере от «работника банка», закончите разговор и перезвоните в банк самостоятельно.

- при онлайн-оплате, в том числе услуг такси, проверяйте адрес сайта и по возможности используйте отдельную карту (виртуальную), на которой храните небольшие суммы.